

The University of Chicago

INTEGRAL DOMAINS IN QUARTIC FIELDS

A PART OF A DISSERTATION SUBMITTED TO
THE FACULTY OF THE DIVISION OF THE
PHYSICAL SCIENCES IN CANDIDACY FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS
AUGUST, 1941

By
FRANK L. MARTIN

CHICAGO, ILLINOIS

1943

The University of Chicago

INTEGRAL DOMAINS IN QUARTIC FIELDS

A PART OF A DISSERTATION SUBMITTED TO
THE FACULTY OF THE DIVISION OF THE
PHYSICAL SCIENCES IN CANDIDACY FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS
AUGUST, 1941

By
FRANK L. MARTIN

CHICAGO, ILLINOIS

1943

TABLE OF CONTENTS

Chapter	Page
INTRODUCTION	1
I. NOTATIONS AND PRELIMINARY RESULTS	3
II. SOLUTIONS OF CONGRUENCES WHEN p IS PRIME TO ab . . .	7
III. SOLUTION OF CONGRUENCES FOR THE CASE WHERE p DIVIDES ab UNDER THE HYPOTHESES IMPLYING $\alpha = 0$	27
IV. CONGRUENCE SOLUTIONS UNDER THE HYPOTHESIS THAT p DIVIDES a AND c BUT NOT b	28
V. SOLUTIONS OF CONGRUENCES WHEN $p \neq 2$ DIVIDES b BUT NOT ac	43
VI. CONGRUENCE SOLUTIONS WHEN $p \neq 2$ DIVIDES BOTH a AND b	46
VII. THE FINAL CASE $p = 2$	49





Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41533907_0053

INTEGRAL DOMAINS IN QUARTIC FIELDS

INTRODUCTION

The problem considered here arises from that of determining integral bases of all quartic fields F over the field R of rational numbers. Let θ be a complex root of an equation $f(x) = 0$ of degree n , coefficients in R , and irreducible in R . Then the integers of F are known¹ to have a basis of the form

$$\omega_1 = 1, \quad \omega_i = \frac{e_{i1} + e_{i2} \theta + \dots + e_{i,i-1} \theta^{i-2} + \theta^{i-1}}{E_i}$$

$$(i = 2, \dots, n).$$

This means that every integer of F is uniquely expressible in the form $c_1 \omega_1 + \dots + c_n \omega_n$ for rational integral c_i . Here the e_{ij} , E_i are rational integers such that E_i divides the discriminant of $f(x)$ and is divisible by E_{i-1} for $i = 2, \dots, n$. The problem mentioned above is thus that of finding the e_{ij} and E_i in terms of the coefficients of the given $f(x)$ and has been solved for² $n = 3$. We are then considering the case $n = 4$.

It has been shown that $f(x)$ may be taken to be a fundamental polynomial³ and such that⁴ necessarily $\omega_2 = \theta$. This, in

¹W. E. H. Berwick, Integral bases. London: Cambridge University Press, 1927, pp. 1-95. See p. 10.

²A. A. Albert, Normalized integral bases of algebraic number fields I, Annals of Mathematics, (2), vol. 38 (1937), pp. 923-57.

³Ibid., p. 932.

⁴Ibid., p. 936.

the quartic case, means that we take

$$f(x) = x^4 + ax^2 + bx + c,$$

where a, b, c are integers such that the congruences $a \equiv 0(p^2)$, $b \equiv 0(p^3)$, $c \equiv 0(p^4)$ do not simultaneously hold for $p > 1$, and with further restrictions implying the non-existence of a simultaneous solution x of

$$f(x) \equiv 0(2^4), f'(x) \equiv 0(2^3), f^{(2)}(x) \equiv 0(2^3).$$

It is known that when this has been done a first part of the finding of the ω_1 is the determination of a maximal integral domain⁵ with a basis of the form

$$1, \theta, \theta^2, \Omega = \frac{(e^3 + ae + b) + (e^2 + a)\theta + e\theta^2 + \theta^3}{E}$$

This problem is equivalent to the determination of e and the maximal integer E for which a simultaneous solution $x = e$ of the congruences

$$f(x) \equiv 0(E^2), f'(x) \equiv 0(E)$$

exists. We shall solve this latter question here and thus complete an important first step in the determination of the integers of all quartic fields over R .

For reference to the equations and theorems of this thesis, we adopt a system used in recent standard texts⁶ in mathematics. We shall number the equations and theorems in each chapter separately, and after the chapter in which they first occur, refer to them by a number consisting of the chapter number and the number of the equation or theorem.

⁵Ibid., p. 938.

⁶See, for example, A. A. Albert, Modern higher algebra, The University of Chicago Press, 1937, p. 1.

CHAPTER I

NOTATIONS AND PRELIMINARY RESULTS

Our problem is the determination of the maximum E for which

$$(1) \quad \begin{aligned} f(x) &= x^4 + ax^2 + bx + c \equiv O(E^2), \\ f'(x) &= 4x^3 + 2ax + b \equiv O(E) \end{aligned}$$

have a simultaneous solution $x = e$. Here $f(x)$ is a fundamental polynomial, that is, it has the property that a, b, c are rational integers such that if $a \equiv O(p^2)$, $b \equiv O(p^3)$, $c \equiv O(p^4)$ for an integer p , then $p = \pm 1$. Further we assume that $f(x)$ is irreducible in $\mathbb{R}$ and satisfies the normalization condition stated in the introduction.

Suppose that the desired number E be expressed as a prime-power product, that is, in the form $E = \prod p_i^{\lambda_i}$. Then (1) implies that the congruences $f(x) \equiv O(p_i^{2\lambda_i})$, $f'(x) \equiv O(p_i^{\lambda_i})$ have a solution $x = e$. Conversely, if a solution $x = e_i$ of these pairs of congruences exists for every i and λ_i a maximum, we may obtain the solution e of (1) by choosing $e \equiv e_i(p_i^{2\lambda_i})$, according to the usual method of the Chinese remainder theorem. The corresponding denominator E will evidently be a maximum. We are then led to determine the maximum value of λ for which there exists a simultaneous solution $x = e$ of the pair of congruences

$$(2) \quad f(x) \equiv O(p^{2\lambda}), \quad f'(x) \equiv O(p^\lambda),$$

where p is a prime.

The discriminant of $f(x)$ is the polynomial

$$(3) \quad D = 16c(a^2 - 4c)^2 - b^2(27b^2 + 4a^3) + 144acb^2$$

in its coefficients. Define

$$(4) \quad g(x) = 4f(x) - xf'(x) = 2ax^2 + 3bx + 4c,$$

so that, by the Division Algorithm,

$$(5) \quad a^2f'(x) = (2ax - 3b)g(x) + r(x),$$

where $r(x)$ is a linear function of x . Then direct computation gives

$$(6) \quad r(x) = Ax + B, \quad A = 9b^2 + 2a^3 - 8ac, \quad B = b(12c + a^2).$$

We shall use the identities (4) and (5) frequently, as well as certain other identities which we shall now derive. The first of these is a consequence of (4), (5) and is given by

$$(7) \quad 4a^2f(x) = (2ax^2 - 3bx + a^2)g(x) + xr(x).$$

This may be rewritten in the form

$$(8) \quad 4a^2f(x) = -3[g(x)]^2 + Bb^{-1}g(x) + x[r(x) + 2h(x)g(x)],$$

where

$$(9) \quad h(x) = 4ax + 3b.$$

We also clearly have

$$(10) \quad 8ag(x) = [h(x)]^2 - (A - 2ab^{-1}B).$$

By direct computation we obtain

$$(11) \quad a^2D = 4cA^2 - 3bAB + 2aB^2,$$

and thus also

$$(12) \quad 8a^3D = (3bA - 4aB)^2 - A^2(A - 2ab^{-1}B).$$

But (11) implies

$$(13) \quad a^2_D = A^2_g(x) - Ah(x)r(x) + 2a[r(x)]^2.$$

The form of (12) then leads us to

$$(14) \quad 3bA - 4aB = Ah(x) - 4ar(x).$$

We finally define

$$(15) \quad F_0(x) = Ah(x) [4a^2 f(x)].$$

Then (7) and (13) imply

$$(16) \quad F_0(x) = Ag(x) [2a^2 f'(x) - 3bg(x) + r(x)] + 2ax[r(x)]^2 - a^2 xD.$$

This is the last of the set identities we have derived here.

If p is a prime for which (2) has a solution with $\lambda > 0$, then the residual polynomials of $f(x)$ and $f'(x)$ in the finite field of p elements have a non-constant factor in common. But this is true if and only if p divides D . Hence we need consider only prime divisors p of D . Let then

$$(17) \quad D = p^\delta D_0, \quad \delta > 0,$$

where D_0 is prime to p . Then $\delta = 2\gamma$ or $\delta = 2\gamma + 1$, where γ is a uniquely determined positive integer. We also write

$$(18) \quad A = p^\alpha A_0, \quad B = p^\beta B_0,$$

where $A_0 B_0$ is prime to p .

Let now $x = e$ be a solution of (2) for $\lambda > 0$ a maximum. Then $f(e) \equiv f'(e) \equiv 0(p^\lambda)$ so that by (4), (5)

$$(19) \quad g(e) \equiv r(e) \equiv 0(p^\lambda).$$

We shall use this result frequently. Note finally, that we shall employ the terminology exactly divisible according to the usual definition⁷ of this phrase.

⁷Albert, Normalized integral bases of algebraic number fields I, op. cit., p. 924.

CHAPTER II

SOLUTION OF CONGRUENCES WHEN p IS PRIME TO ab

1. General results. If p is prime to ab and $\alpha > 0$ in (1:18), equation (1:11) implies also $\beta > 0$. Hence we may prove

LEMMA 1. Let p be prime to ab and such that $\alpha > 0$.

Then $p \neq 3$, and $c \not\equiv 0(p)$.

For proof, we see that (1:6) with $c \equiv 0(p)$ leads to $B \equiv ba^2(p) \not\equiv 0(p)$, a contradiction. Likewise $B = b(12c + a^2) \equiv ba^2(3)$, so that $p \neq 3$ and our lemma is proved.

By (1:11), a^2D is a quadratic form in A and B with coefficients prime to p . But then we clearly have

LEMMA 2. If $\alpha \neq \beta$, then $\delta = 2\gamma$, γ is the lesser of α, β . Moreover if $\delta = 2\gamma + 1$, then $\beta = \alpha \leq \gamma$.

These results will be used throughout the remainder of this chapter.

2. Consequences of the property $0 < 3\alpha < \delta$. By Lemma 2 and the hypothesis of this section we clearly have the result

$\beta = \alpha$. Hence the term $A - 2ab^{-1}B$ appearing in (1:12) is divisible by p^α . Moreover this divisibility is exact, for we obviously have $3bA - 4aB \equiv 0(p^{\alpha+1})$, which is incompatible with $A - 2ab^{-1}B \equiv 0(p^{\alpha+1})$. We may therefore write

$$(1) \quad A - 2ab^{-1}B = Cp^\alpha, \quad C \not\equiv 0(p),$$

for the integral C . Then by (1:12) and (1:17)

$$(3bA - 4aB)^2 \equiv CA_0^2 p^{3\alpha} \pmod{p^6},$$

so that we have as an immediate consequence

THEOREM 1. The integer α is even, and

$$(2) \quad 3bA - 4aB = Gp^{3\alpha/2}, \quad G \not\equiv 0(p),$$

for integral G.

Let us now define the integer⁸

$$(3) \quad \lambda_0 = \left[\frac{\delta - \frac{3\alpha}{2}}{2} \right],$$

and establish

LEMMA 3. The integer λ has λ_0 as a lower bound. A corresponding solution $x = e$ of (1:2) may be obtained by choosing e to be a solution of

$$(4) \quad r(x) \equiv 0(p^\delta).$$

For we select e by (4). Then from (1:13) we see that $g(e) \equiv 0(p^{\delta-2\alpha})$, while (1:14) and (2) imply $h(e) \equiv 0(p^{\alpha/2})$. Thus it follows from (1:5), (1:8) that $a^2 f'(e) \equiv 0(p^{\delta-2\alpha})$, $4a^2 f(e) \equiv 0(p^{\delta-3\alpha/2})$ and our lemma is proved.

We shall improve this lower bound by means of

THEOREM 2. The integer $\lambda \geq \alpha$. Equations (1:2) may be satisfied for $\lambda = \alpha$ by choosing the solution $x = e$ in the form

$$(5) \quad e = e_0 + kp^{\alpha/2}.$$

The integer e_0 of (5) is given as a solution of

$$(6) \quad r(x) \equiv 0(p^{3\alpha/2+1}),$$

while k must be taken as a solution of

$$(7) \quad 4ax + 3h_0 \equiv 0(p),$$

⁸Throughout this thesis Greek letters will represent exponents of the prime p . Whenever the bracket symbol encloses a Greek letter it is to be read "the greatest integer" in the enclosed expression. In all other contexts the symbol called a bracket has its usual meaning.

with h_0 defined by $h(e_0) = h_0 p^{\alpha/2}$.

In proof, take e_0 to be a solution of (6). We then write $r(e_0) = r_0 p^{3\alpha/2+1}$. Equations (1:13), (1:14) and (2) enable us to write also $g(e_0) = g_0 p^{\alpha+1}$, $h(e_0) = h_0 p^{\alpha/2}$, $h_0 \not\equiv 0(p)$, for quotients g_0, h_0 . Finally, let us write e in the form (5) and assume $k \not\equiv 0(p)$. We shall determine an e of this form for which (1:2) is satisfied with $\lambda = \alpha$.

For e as given by (5), (6), we clearly have $g(e) \equiv 0(p^\alpha) \not\equiv 0(p^{\alpha+1})$. Hence by (1:8), $4a^2 f(e) \equiv e[r(e) + 2h(e)g(e)] \pmod{p^{2\alpha}}$, with $e \not\equiv 0(p)$. Consequently $f(e) \equiv 0(p^{2\alpha})$ if and only if $x = e$ satisfies

$$(8) \quad H(x) = r(x) + 2h(x)g(x) \equiv 0(p^{2\alpha}).$$

But then $H(e)$ may be developed in a Taylor series as in

$$(9) \quad H(e) = H(e_0) + H'(e_0)kp + \frac{H^{(2)}(e_0)}{2!}k^2p^2 + \frac{H^{(3)}(e_0)}{3!}k^3p^3,$$

where $\sigma = \alpha/2$, and

$$(10) \quad \begin{aligned} H(e_0) &= r(e_0) + 2h(e_0)g(e_0), \\ H'(e_0) &= A + 2[h(e_0)]^2 + 8ag(e_0) = 24ag(e_0) + (3A - 4ab^{-1}B), \\ \frac{H^{(2)}(e_0)}{2!} &= 12ah(e_0), \quad \frac{H^{(3)}(e_0)}{3!} = 16a^2, \end{aligned}$$

and where the second form of $H'(e_0)$ results from its first form by use of (1:10). Making the substitutions described for $r(e_0)$, $g(e_0)$, $h(e_0)$ in (10) we obtain

$$(11) \quad \begin{aligned} H(e_0) &= (r_0 + 2g_0h_0)p^{3\sigma+1}, \quad H'(e_0) = 24ag_0p^{2\sigma+1} + b^{-1}g_0p^{3\sigma}, \\ \frac{H^{(2)}(e_0)}{2!} &= 12ah_0p^\sigma, \quad \frac{H^{(3)}(e_0)}{3!} = 16a^2. \end{aligned}$$

Then the substitution of (11) in (9) yields

$$(12) \quad H(e) = p^3 \sigma [r_0 + 2h_0 g_0] p + (24a g_0 p + b^{-1} g p^\sigma) k \\ + 12ah_0 k^2 + 16a^2 k^3.$$

Let us now designate by $G(k)$ the expression within the bracket in (12). Then if we choose k to satisfy (7), we have

$$G(k) = 4ak^2(4ak + 3h_0) \equiv 0(p).$$

Obviously then k satisfies $k \not\equiv 0(p)$ so that $G'(k) \not\equiv 0(p)$ is also true. We now make use of a well known theorem of elementary

number theory which states, in effect, that if a polynomial

$\Phi(x) \equiv 0(p)$ has a solution k for which $\Phi'(k) \not\equiv 0(p)$, then

$\Phi(x) \equiv 0(p^\mu)$ has a solution for every μ . Hence we may conclude that $G(k) \equiv 0(p^\sigma)$ has a solution and consequently $H(e) \equiv 0(p^{2\alpha})$.

Note finally that $f(e) \equiv 0(p^{2\alpha})$, $g(e) \equiv 0(p^\alpha)$ imply $f'(e) \equiv 0(p^\alpha)$, so that our proof is complete.

We now define

$$(13) \quad \lambda_1 = \max (\lambda_0, \alpha).$$

Then Lemmas 3 and 4 imply the trivial

LEMMA 5. The inequality $\lambda \geq \lambda_1$ holds.

We now investigate the conditions under which $\lambda > \lambda_1$ and shall prove

LEMMA 6. A necessary and sufficient condition that (1:2) be satisfied with $\lambda > \lambda_1$ is given by

$$(14) \quad F(e) = 16A[g(e)]^2 + 2[r(e)]^2 - aD \equiv 0(p^{2\lambda+3\alpha/2}), \\ g(e) \equiv 0(p^\lambda).$$

For, we have already seen that $f(e) \equiv 0(p^{2\lambda})$, $f'(e) \equiv 0(p^\lambda)$ imply $g(e) \equiv 0(p^\lambda)$. We shall have proved our result when we show

that the first of (14) is equivalent to $f(e) \equiv O(p^{2\lambda})$. The hypothesis $\lambda > \lambda_1 \geq \alpha$ implies, by (1:10), that $h(e) \equiv O(p^{\alpha/2}) \not\equiv O(p^{\alpha/2+1})$. Consequently, from (1:6) the function $F_0(e) \equiv O(p^{2\lambda+3\alpha/2})$. But then the condition $g(e) \equiv O(p^\lambda)$ combined with (1:13) implies that $r(e) \equiv O(p^{\lambda+3\alpha/2})$.

The first part of $F_0(e)$ as given in (1:16) is

$$Ag(e)[2a^2f'(e) - 3bg(e) + r(e)].$$

This expression may be rewritten in the form

$Ag(e)[h(e)g(e) + 3r(e) - 12bg(e)]$, which, in view of our previous condition on $g(e)$, is congruent mod $p^{2\lambda+3\alpha/2}$ to $-12bA[g(e)]^2$.

Hence we have the result

$$(15) F_0(e) \equiv -12bA[g(e)]^2 + 2ae[r(e)]^2 - a^2eD \pmod{p^{2\lambda+3\alpha/2}}.$$

We shall now establish the upper bound on λ as given by $\lambda \leq \gamma - \alpha/2$. For, if $\lambda = \lambda_2 = \gamma - \alpha/2 + 1$, we would have by (1:19) $g(e) \equiv O(p^{\lambda_2})$, and by (1:13), $r(e) \equiv O(p^{\lambda_2+\alpha/2})$. Thus by (15), $F_0(e) \equiv -a^2eD \pmod{p^{2\gamma+2}}$, $F_0(e)$ is exactly divisible by p^δ , a contradiction.

Let us now form $4F_0(e)$. Then $h(e) \equiv O(p^{\alpha/2})$ implies $8ae[r(e)]^2 \equiv -6b[r(e)]^2$, and $-4a^2eD \equiv 3baD \pmod{p^{2\lambda+3\alpha/2}}$. Consequently,

$$4F_0(e) \equiv -3b\{16A[g(e)]^2 + 2[r(e)]^2 - aD\} \pmod{p^{2\lambda+3\alpha/2}},$$

so that if $g(e) \equiv O(p^\lambda)$, then $F_0(e) \equiv O(p^{2\lambda+3\alpha/2})$ if and only if the first of equations (14) is satisfied.

We have, incidentally, proved

LEMMA 7. An upper bound on λ is given by $\lambda \leq \gamma - \alpha/2$.

In fact if $\lambda > \lambda_1$ and if we determine e so that

$$(16) \quad g(e) = g \cdot p^{\xi}, \quad (g, p) = 1,$$

holds, then $\lambda \leq \xi \leq \gamma - \frac{\alpha}{2}$.

When (16) holds we have, in addition,

$$(17) \quad r(e) = rp^{\xi+\alpha/2}, \quad r \neq 0(p),$$

$$(18) \quad h(e) = hp^{\alpha/2}, \quad h \neq 0(p),$$

for quotients r, h . We may then prove the auxiliary

LEMMA 8. If $\lambda > \alpha$, then

$$(19) \quad r + 2gh \equiv 0(p).$$

For, from (1:13) with $x = e$ we have on substitution from (16), (17), (18) the identity $A_0(A_0g - rh)p^{\xi+2\alpha} + 2ar^2p^{2\xi+\alpha} = a^2D_0p^{\delta}$ and thus

$$A_0(A_0g - rh) + 2ar^2p^{\xi-\alpha} = a^2D_0p^{\delta-\xi-2\alpha}.$$

Multiplying the last equation by $2h$, we obtain

$$(20) \quad A_0(2A_0gh - r \cdot 2h^2) + 4ar^2hp^{\xi-\alpha} = 2ha^2D_0p^{\delta-\xi-2\alpha}.$$

But then as a consequence of (1:10) and (1), we have $h^2 - c = 8agp^{\xi-\alpha}$, while (1) and (2) imply $2c = b^{-1}Gp^{\alpha/2} - A_0$.

Combining these two results we have

$$(21) \quad 2h^2 = b^{-1}Gp^{\alpha/2} + 16agp^{\xi-\alpha} - A_0.$$

Then (21) combined with (20) yields

$$(22) \quad \begin{aligned} A_0^2(r + 2gh) - A_0rb^{-1}Gp^{\frac{\alpha}{2}} - 4arp^{\xi-\alpha}(4A_0g - rh) \\ = 2ha^2D_0p^{\delta-\xi-2\alpha}. \end{aligned}$$

Our result then follows at once from (18) in view of

$$\xi \geq \lambda > \alpha.$$

Making use of Lemma 8, we shall prove

LEMMA 9. The inequality $\lambda > \lambda_1$ holds only if $\delta = 2\gamma$ and $\varepsilon = \gamma - \alpha/2$ in (16).

For proof, we first multiply $F(e)$ of (14) by A , whence substitution for $A^2g(e)$ from (1:13) yields

$$\begin{aligned} AF(e) &= 16g(e)\{a^2D + Ah(e)r(e) - 2a[r(e)]^2\} + 2A[r(e)]^2 - aAD \\ &= 2Ar(e)[r(e) + 8h(e)g(e)] + 16a^2Dg(e) - 32ag(e)[r(e)]^2 - aAD. \end{aligned}$$

Substitution in the latter from (16), (17), (18) leads to

$$\begin{aligned} (23) \quad AF(e) &= 2A_0r(r + 8hg)p^{\varepsilon+2\alpha} + 16a^2gD_0p^{\delta+\varepsilon} \\ &\quad - 32agr^2p^{3\varepsilon+\alpha} - A_0aD_0p^{\delta+\alpha}. \end{aligned}$$

In view of $\lambda > \lambda_1 \geq \lambda_0$ and Lemma 6 we have

$$(24) \quad AF(e) \equiv O(p^{\delta+1+\alpha}).$$

But then, by Lemma 8, it follows that $r + 2gh \equiv O(p)$ and hence that $r + 8gh \equiv 6gh \not\equiv O(p)$. Accordingly (23) may be satisfied mod $p^{\delta+1+\alpha}$ if and only if $2\varepsilon + 2\alpha = \delta + \alpha$, or

$$(25) \quad 2\varepsilon = \delta - \alpha.$$

Equation (25) is possible if and only if $\delta = 2\gamma$. Consequently when $\delta = 2\gamma + 1$ we cannot have $\lambda > \lambda_1$, and we state this result in

THEOREM 3. Let $\delta = 2\gamma + 1$. Then λ is the maximum of α and λ_0 given by (3).

We have now reduced the problem to the case $\delta = 2\gamma$ and shall prove as the final result of this section

THEOREM 4. Let $\delta = 2\gamma$. Then the integer $\lambda = \gamma - \alpha/2$ if and only if $-6aD_0$ is a quadratic residue of p . In this case, we solve equations (1:2) by choosing $x = e$ in the form

$$(26) \quad e = e_0 + kp^{\gamma-\alpha}$$

with e_0 the unique solution mod $p^{\gamma-\alpha}$ of

$$(27) \quad A_0x + B_0 \equiv 0(p^{\gamma-\alpha}),$$

and k satisfying

$$(28) \quad y^2 \equiv -6aD_0(p), \quad y = 6A_0k - 2(r_0 + 8g_0h_0).$$

If $-6aD_0$ is a quadratic non-residue of p , then λ is the maximum of α and λ_0 . In this case, if $\alpha \geq \lambda_0$, we solve (1:2) by taking $x = e$ to be a solution of

$$(29) \quad r(x) \equiv 0(p^{3\alpha/2}) \not\equiv 0(p^{3\alpha/2+1}),$$

while if $\lambda_0 > \alpha$, we take e to be a solution of

$$(30) \quad r(x) \equiv 0(p^\delta).$$

In proof, we saw by Lemma 9 that the integer $\lambda > \lambda_1$ only if $\varepsilon = \gamma - \alpha/2$ in equations (16), (17). Let us choose e_0 to be the unique solution mod $p^{\gamma-\alpha}$ of (27). In a similar manner to the first result of the first paragraph of Theorem 2, we then have

$$(31) \quad r(e_0) = r_0p^\gamma, \quad g(e_0) = g_0p^{\gamma-\alpha/2}, \quad h(e_0) = h_0p^{\alpha/2}, \quad h_0 \not\equiv 0(p).$$

Write $e = e_0 + kp^\mu$, $\mu = \gamma - \alpha$. Then $F(e)$ of (14) may be developed in a Taylor expansion of the form

$$(32) \quad \begin{aligned} F(e) = & F(e_0) + F'(e_0)kp^\mu + \frac{F^{(2)}(e_0)}{2!}k^2p^{2\mu} \\ & + \frac{F^{(3)}(e_0)}{3!}k^3p^{3\mu} + \frac{F^{(4)}(e_0)}{4!}k^4p^{4\mu}, \end{aligned}$$

where

$$\begin{aligned}
 F(e_0) &= 16A[g(e_0)]^2 + 2[r(e_0)]^2 - aD, \\
 F'(e_0) &= 4A[r(e_0) + 8h(e_0)g(e_0)], \\
 (33) \quad \frac{F^{(2)}(e_0)}{2!} &= 2A^2 + 16A[h(e_0)]^2 + 64Ag(e_0) \\
 &= 3 \cdot 2^6 aAg(e_0) + 8b^{-1}AGp^{3\alpha/2} - 6A^2, \\
 \frac{F^{(3)}(e_0)}{3!} &= 2^6 Aah(e_0), \quad \frac{F^{(4)}(e_0)}{4!} = 2^6 Aa^2,
 \end{aligned}$$

and where, in computing the second form of $F^{(2)}(e_0)/2!$, we have used (1:10). Making the substitution of (31) in (33) yields

$$\begin{aligned}
 F(e_0) &= p^{2\gamma}Q, \quad Q = 16A_0g_0^2 + 2r_0^2 - aD_0, \\
 F'(e_0) &= 4A_0(r_0 + 8h_0g_0)p^{\gamma+\alpha}, \\
 (34) \quad \frac{F^{(2)}(e_0)}{2!} &\equiv 3 \cdot 2^6 aA_0g_0p^{\gamma+\alpha/2} - 6A_0^2p^{2\alpha} \pmod{p^{5\alpha/2}}, \\
 \frac{F^{(3)}(e_0)}{3!} &= 2^6 A_0ah_0p^{3\alpha/2}, \quad \frac{F^{(4)}(e_0)}{4!} = 2^6 a^2A_0p^\alpha.
 \end{aligned}$$

Combining (34) with (32), we have

$$(35) \quad F(e) \equiv p^{2\gamma} \left\{ [-6A_0k^2 + 4A_0(r_0 + 8h_0g_0)k + Q] + 2^6 aA_0k^2p^{\gamma-3\alpha/2}(3g_0 + kh_0 + p^{\gamma-3\alpha/2}ak^2) \right\} \pmod{p^{2\gamma+\alpha/2}}.$$

Let us designate by $G(k)$ the expression within the braces in (28).

Then evidently

$$(36) \quad G(k) \equiv -6A_0k^2 + 4A_0(r_0 + 8h_0g_0)k + Q \pmod{p}.$$

Multiply $G(k)$ by -6 . Then if we substitute the value of Q from the first of equations (34), we have

$$(37) \quad -6G(k) \equiv [6A_0k - 2(r_0 + 8g_0h_0)]^2 - 2[8(r_0 + 2g_0h_0) + 3 \cdot 2^4 ag_0^2(A_0 + 2h_0^2) - 3aD_0] \pmod{p}.$$

Moreover from (1:10), $h_0^2 = 3ag_0p^{\gamma-3\alpha/2} + C$, while from (1), (2) we have

$$A_0 + 2C = b^{-1}Gp^{\alpha/2}.$$

Thus $A_0 + 2h_0^2 = 16ag_0p^{\gamma-3\alpha/2} + b^{-1}g_0p^{\alpha/2} \equiv 0(p)$. Also, by Lemma 8, it follows that $r_0 + 2g_0h_0 \equiv 0(p)$. Consequently, if we write $6A_0k - 2(r_0 + 8g_0h_0) = y$, (30) implies

$$(38) \quad -6G(k) \equiv y^2 + 6aD_0(p).$$

Clearly (38) may be solved if and only if $-6aD_0$ is a quadratic residue of p , and the solution y , if it exists is prime to p . Also $-6G'(k) \equiv 2y \cdot 6A_0 \not\equiv 0(p)$, and so by application of the theorem referred to on page 10, we may solve $G(k) \equiv 0(p^{\alpha/2})$. Thus (35) implies that $F(e) \equiv 0(p^{2\gamma+\alpha/2})$, so that $\lambda = \gamma - \alpha/2$. However if $-6aD_0$ is a quadratic non-residue of p , we have $G(k) \not\equiv 0(p)$, and (35) implies $F(e) \equiv 0(p^{2\gamma}) \not\equiv 0(p^{2\gamma+1})$, or $\lambda = \lambda_0$. This completes our proof.

3. Properties for the case $\delta = 3\alpha$. Our hypothesis evidently implies

LEMMA 10. The integer $\beta = \alpha$, $\alpha \equiv \beta \equiv \delta(2)$.

For, if $\delta = 2\gamma = 3\alpha$, we clearly have $\alpha < \gamma$, so that Lemma 2 implies the result for this case. When $\delta = 2\gamma + 1$, Lemma 2 states that $\alpha = \beta \leq \gamma$.

As a result of this lemma and the fact that (1:12) implies $3bA - 4aB \equiv 0(p^{\alpha+1})$, we again have (1). But then (1:12) and the hypothesis $3\alpha = \delta$ yield the result

$$(39) \quad (3bA - 4aB)^2 = (8a^3D_0 + A_0^2C)p^\delta.$$

The form of (39) then clearly requires

$$(40) \quad 8a^3D_0 + A_0^2C = G_0^2p^f, \quad G_0 \not\equiv 0(p), \quad f \geq 0,$$

where f has the form 2ν or $2\nu + 1$ according as δ is even or odd. Let us now define

$$(41) \quad \delta_0 = \left[\frac{\delta + 1}{2} \right].$$

We then have $\delta_0 = \gamma$ when δ is even, $\delta_0 = \gamma + 1$ when δ is odd, and (39), (40), (41) evidently imply the result which we shall state in

THEOREM 5. The equation

$$(42) \quad 3bA - 4aB = G_0 p^{\delta_0 + \nu}, \quad G_0 \not\equiv 0(p), \quad \nu \geq 0,$$

holds for G_0, ν , as defined in (40), δ_0 in (41).

We shall now establish an upper bound on λ by proving

LEMMA 11. The integer $\lambda \leq \alpha$.

If δ is odd (1:10), (1) imply the desired result immediately, for then by Lemma 10, α is odd and the condition $g(e) \equiv 0(p^{\alpha+1})$ is impossible. But if $\delta \equiv \alpha \equiv 0(2)$, then $g(e) \equiv 0(p^{\alpha+1})$ implies $h(e) \equiv 0(p^{\alpha/2}), \not\equiv 0(p^{\alpha/2+1})$, by (1:10). Also, from (1:13), we have $r(e) \equiv 0(p^{3\alpha/2}) \not\equiv 0(p^{3\alpha/2+1})$. Accordingly, (1:8) yields the result $4a^2f(e) \equiv 0(p^{3\alpha/2}) \not\equiv 0(p^{3\alpha/2+1})$ and our lemma is proved.

We now define the quantity

$$(43) \quad \lambda_0 = \left[\frac{\gamma}{2} \right],$$

and shall prove

LEMMA 12. The integer $\lambda > \lambda_0$ only if $x = e$ satisfies

$$(44) \quad h(x) \equiv 0(p^\sigma), \quad \sigma = \left[\frac{\alpha + 1}{2} \right].$$

For, if we take e to be a solution of $h(x) \equiv 0(p^{\sigma_0})$, $\sigma_0 < \sigma$, then (1:10) clearly implies $g(e) \equiv 0(p^{2\sigma_0}), \not\equiv 0(p^{2\sigma_0+1})$, while (1:14), (42) require $r(e) \equiv 0(p^{\alpha+\sigma_0}), \not\equiv 0(p^{\alpha+\sigma_0+1})$. But these results when inserted in (1:9) show that $4a^2f(e) \equiv 0(p^{3\sigma_0}) \not\equiv 0(p^{3\sigma_0+1})$, $3\sigma_0 \leq 3[(\alpha - 1)/2]$, so that λ for this choice of e

would satisfy the inequality $2\lambda \leq 3[(\alpha - 1)/2] < \gamma$, a contradiction.

We now have, as an immediate consequence of Lemma 12 and the fact that $\lambda \leq \alpha$,

LEMMA 13. The maximum integer λ satisfying (1:2) is identical with that satisfying

$$(45) \quad \begin{aligned} H(x) = r(x) + 2h(x)g(x) &\equiv 0(p^{2\lambda}), \\ g(x) &\equiv 0(p^\lambda). \end{aligned}$$

The second of equations (45) is an immediate consequence of (44), while the first equation of (45) then follows at once from (1:9).

We proceed now to our actual determination of λ . Let e_0 be the unique solution mod p^σ of (44), so that we have

$$(46) \quad h(e_0) = h_0 p^\sigma, \quad g(e_0) = g_0 p^\alpha, \quad r(e_0) = r_0 p^{\alpha+\sigma}.$$

The second of (46) has been obtained by means of the first of (46) together with (1:10), while the third of (46) results from the first in (1:14). In fact (46) applied to (1:14), (42) yields

$$3bA - 4aB = (A_0 h_0 - 4a r_0) p^{\alpha+\sigma} = G_0 p^{\delta_0+\nu}.$$

Then since $\sigma = [(\alpha + 1)/2]$, we have $\delta_0 = \alpha + \sigma$, and consequently

$$(47) \quad 4a_0 r_0 = A_0 h_0 - G_0 p^\nu$$

holds. If now we write

$$(48) \quad e = e_0 + kp^\sigma,$$

we have the latter as the most general solution of (44). We may then develop $H(e)$ in a Taylor series as in (9), (10).

Substitution of (46) in (10) yields

$$(49) \quad H(e_0) = (r_0 + 2g_0h_0)p^{\alpha+\sigma}, \quad H'(e_0) = (A_0 - C + 3h_0^2p^{2\sigma-\alpha})p^\alpha,$$

$$\frac{H^{(2)}(e_0)}{2!} = 12ah_0p^\sigma, \quad \frac{H^{(3)}(e_0)}{3!} = 16a^2.$$

The result of (49) in (9) is given by

$$(50) \quad H(e) = p^{\sigma+\alpha} \left\{ (r_0 + 2h_0g_0) + (A_0 - C + 3h_0^2p^\mu)k + 12ah_0k^2p^\mu + 16a^2k^3p^\mu \right\}, \quad \mu = 2\sigma - \alpha.$$

Let us now call the expression within the braces in (50) $G(k)$.

Multiplying $G(k)$ by $4a$, we obtain

$$(51) \quad 4aG(k) = 4ar_0 + h_0 \cdot 8ag_0 + (A_0 - C)4ak + 12akh_0^2p^\mu + 48a^2h_0k^2p^\mu + 64a^3k^3p^\mu.$$

Moreover, we have as a result of (1:10),

$$(52) \quad 8ag_0 = h_0^2p^\mu - C.$$

Consequently, substitution for $8ag_0$ from (52) and for $4ar_0$ from (47), and subsequent regrouping of terms leads us to

$$(53) \quad 4aG(k) = -G_0p^\nu + (A_0 - C)(4ak + h_0) + p^\mu(4ak + h_0)^3.$$

Moreover, combining (1) and (42), we see that

$$(54) \quad A_0 + 2C = b^{-1}G_0p^{\sigma+\nu}$$

is true, and hence $A_0 - C = b^{-1}G_0p^{\sigma+\nu} - 3C$. Accordingly if we write

$$(55) \quad 4ak + h_0 = y,$$

(53) becomes

$$(56) \quad 4aG(k) \equiv -G_0p^\nu - 3Cy + p^\mu y^3(p^\sigma).$$

We are now able, by means of (49), to proceed rather simply to our final results. Suppose first that $\delta = 2\gamma$, so that α even requires $\sigma = \alpha/2$. Then $\mu = 2\sigma - \alpha = 0$, and we have

$$(57) \quad 4aG(k) \equiv -G_0p^\nu - 3Cy + y^3(p^\sigma).$$

If further $\nu = 0$, then $G(k) \equiv 0(p)$ if and only if the equation

$$(58) \quad M(y) = y^3 - 3Cy - G_0 \equiv 0(p),$$

has a solution $y \bmod p$. But then we shall prove

LEMMA 14. Let $\delta = 2\gamma$ and $\nu = 0$, where the symbol ν is that of (40). If the function $M(y)$ of (58) satisfies $M(y) \equiv 0(p)$, for a solution $y \bmod p$, then $M'(y) \not\equiv 0(p)$.

For otherwise $M(y) \equiv 0(p)$, $M'(y) \equiv 0(p)$ have a common solution so that the discriminant D_M of $M(y)$ is divisible by p . That is, $D_M = -27(G_0^2 - 4C^3) \equiv 0(p)$, and we have immediately

$$(59) \quad G_0^2 - 4C^3 \equiv 0(p).$$

However, the hypothesis $\delta = 2\gamma$, $\nu = 0$ implies, by (40)

$$(60) \quad G_0^2 = 8a^3D_0 + A_0^2C.$$

Combining (59), (60) we obtain

$$8a^3D_0 + C(A_0 + 2C)(A_0 - 2C) \equiv 0(p),$$

which in view of (54) requires $D_0 \equiv 0(p)$, contrary to the definition of D_0 . Our lemma is thus proved.

Thus in the case $\delta = 2\gamma$, $\nu = 0$, if $M(y) \equiv 0(p)$ has a solution y , then certainly $M'(y) \not\equiv 0(p)$. Consequently, by Lemma 14 the hypothesis $M(y) \equiv 0(p)$ solvable is equivalent to the conclusion $G(k) \equiv 0(p)$, $G'(k) \not\equiv 0(p)$, and hence to the conclusion

that $G(k) \equiv O(p^\sigma)$ is solvable. We then have, by (50), $H(e) \equiv O(p^{2\alpha})$, or $\lambda = \alpha$. However if $M(y) \equiv O(p)$ has no solution, $H(e) \equiv O(p^{3\alpha/2}) \not\equiv O(p^{3\alpha/2+1})$ so that $\lambda = \lambda_0$ in this case.

Suppose now $\delta = 2\gamma$, $\nu > 0$. Then, by (56), $4aG(k) \equiv y^3 - Cy(p)$, from which, by means of (55), $4aG'(k) \equiv (3y^2 - 3C) \cdot 4a \pmod{p}$. It is then obvious that $y \equiv O(p)$ is a simultaneous solution of $G(k) \equiv O(p)$, $G'(k) \not\equiv O(p)$, and hence that $G(k) \equiv O(p^\sigma)$ has a solution for which $y \equiv O(p)$. Again, (50) enables us to conclude that, when $\delta = 2\gamma$, $\nu > 0$, we may always satisfy $H(e) \equiv O(p^{2\alpha})$, so that $\lambda = \alpha$. Combining these results for the case $\delta = 2\gamma$, we have proved

THEOREM 6. Let $\delta = 2\gamma = 3\alpha$. Then if ν is zero, the integer $\lambda = \alpha$ or $\lambda = \lambda_0$ given by (43) according as (58) has or has not a solution mod p . In the latter case the corresponding e may be taken to be a solution of (44), while in the former case we choose e by means of (46), (48), (55), (58). If $\nu > 0$, then $\lambda = \alpha$ and the corresponding e is given by (46), (48), (55) and $y \equiv O(p)$.

We have yet to consider $\delta = 2\gamma + 1$. For this case we shall prove our final result, which we state in

THEOREM 7. If $\delta = 2\gamma + 1 = 3\alpha$, we have $\lambda = \alpha$. The corresponding e is then given by means of (46), (48), (53) and

$$(61) \quad 3Cy + G_0p^\nu \equiv O(p), \quad \nu \geq 0.$$

For, the hypothesis δ odd implies $2\sigma = \alpha + 1$, so that μ defined in (50) has the value unity. Then, by (56), we have

$$4aG(k) \equiv -3Cy - G_0p^\nu(p),$$

and also

$$4aG'(k) \equiv -12aC(p).$$

Accordingly $G(k) \equiv 0(p)$ if and only if y satisfies (61), which always has solutions in view of $3\alpha \not\equiv 0(p)$. Then $G'(k) \not\equiv 0(p)$ implies the solvability of $G(k) \equiv 0(p^\sigma)$, so that by (50) we have $H(e) \equiv 0(p^{2\alpha})$. The proof of Theorem 7 is thus complete.

4. Results for the case $3\alpha > \delta$. In Lemma 2 we showed that either $\alpha = \beta$ with $\gamma \geq \alpha$, or $\alpha \neq \beta$, when γ is the lesser of α and β . If then, we define

$$(62) \quad \alpha_0 = \min(\alpha, \beta),$$

we have at once

LEMMA 15. The number C defined by

$$(63) \quad A - 2ab^{-1}B = c_p^{\alpha_0}$$

is integral.

As a consequence of (1:12) and (63) we clearly have

$$(64) \quad (3bA - 4aB)^2 \equiv 8a^3D_0p^\delta \pmod{p^{3\alpha_0}}.$$

Moreover, $\delta < 3\alpha_0$. For the result just stated is trivial if $\alpha_0 = \alpha$. If $\alpha_0 \neq \alpha$, then $\alpha_0 = \gamma$, and $3\alpha_0 = 3\gamma \not\equiv \delta$ if and only if $\delta = 2\gamma + 1$, and $\gamma = 1$. But then, Lemma 2 states that if $\delta = 2\gamma + 1$, $\alpha = \beta \leq \gamma$. Hence we must have $\alpha = 1$ and thus $3\alpha = \delta$, contrary to the hypothesis of this section. Thus equation (64) implies

$$(65) \quad (3bA - 4aB)^2 \equiv 8a^3D_0p^\delta(p^{\delta+1}),$$

so that we have as a result

THEOREM 8. Let $3\alpha > \delta$. Then $\delta = 2\gamma$ and

$$(66) \quad 3bA - 4aB = Gp^\gamma, \quad G \not\equiv 0(p),$$

holds for integral G . Also the integer $2aD_0$ is a quadratic residue of p .

We shall now establish

LEMMA 16. The integer λ satisfies the inequality

$$\lambda_0 \leq \lambda < \alpha_0, \quad \lambda_0 = \left[\frac{\gamma}{2} \right].$$

For suppose $\lambda = \alpha_0$. A necessary condition then is $g(e) \equiv 0(p^{\alpha_0})$, so that (1:10) and (63) imply $h(e) \equiv 0(p^{\sigma_0})$, $\sigma_0 = [(\alpha_0 + 1)/2]$. We then have $\alpha_0 + \sigma_0 \geq 3\alpha_0/2 > \gamma$, and consequently (1:14), (66) require the condition $r(e) \equiv 0(p^\gamma) \not\equiv 0(p^{\gamma+1})$. These results when introduced into (1:8) imply that $4a^2f(e) \equiv 0(p^\gamma) \not\equiv 0(p^{\gamma+1})$, contradicting $\lambda = \alpha_0$. We have, however, demonstrated that a solution $x = e$ of $h(x) \equiv 0(p^{\sigma_0})$ gives the result $\lambda = \lambda_0$, so that our proof is complete.

We now determine somewhat stronger conditions on e by proving

LEMMA 17. A necessary condition that $\lambda > \lambda_0$ is that e shall be taken to be a root of

$$(67) \quad h(x) \equiv 0(p^\sigma) \not\equiv 0(p^{\sigma+1}), \quad \gamma - \alpha_0 < \sigma \leq \left[\frac{\alpha_0 - 1}{2} \right].$$

We have already seen that, if $\sigma = [(\alpha_0 + 1)/2]$, then $\lambda = \lambda_0$, contradicting $\lambda > \lambda_0$. Hence we have established the upper bound on σ . It remains to be seen that $\lambda > \lambda_0$ implies $\sigma > \gamma - \alpha_0$. Suppose $\sigma \leq \gamma - \alpha_0$. Then by (1:10), (63) and the fact that $\delta = 2\gamma < 3\alpha_0$, we have $g(e) \equiv 0(p^{2\sigma}) \not\equiv 0(p^{2\sigma+1})$. Then (1:14) and (66) imply $r(e) \equiv 0(p^{\alpha_0+\sigma})$. These results introduced into (1:8) lead us to the conclusion $4a^2f(e) \equiv 0(p^{3\sigma}) \not\equiv 0(p^{3\sigma+1})$, and hence $2\lambda \leq 3\sigma \leq 3\gamma - 3\alpha_0 < \gamma$, a contradiction. This completes the proof of Lemma 17.

Suppose next that we take e as in (67). Then

$\alpha_0 + \sigma > \gamma$, and consequently by (1:14), (66) it follows that

$r(e) \equiv 0(p^Y) \not\equiv 0(p^{Y+1})$. In view of (1:10) and the fact that $2\sigma < \alpha_0$, we have clearly $g(e) \equiv 0(p^{2\sigma}) \not\equiv 0(p^{2\sigma+1})$. But then (1:8) implies

$$(68) \quad 4a^2f(e) \equiv e[r(e) + 2h(e)g(e)] \pmod{p^{4\sigma}},$$

where $e \not\equiv 0(p)$ since it satisfies (67) with $ab \not\equiv 0(p)$. Now the second term within the bracket is divisible exactly by $p^{3\sigma}$, while $r(e) \equiv 0(p^Y) \not\equiv 0(p^{Y+1})$. These considerations lead us to

LEMMA 18. We have $\lambda > \lambda_0$ only if $Y \equiv 0(3)$ and we choose the integer σ of (67) to satisfy $Y = 3\sigma$. If $Y \not\equiv 0(3)$, then $\lambda = \lambda_0$ and an appropriate solution $x = e$ of (1:2) is obtained by choosing e to be a solution of (67) with $3\sigma > Y$.

Henceforth let us assume that $3\sigma = Y$. Then since $6\sigma = 2Y < 3\alpha$, we clearly have $2\sigma < \alpha$. Moreover since $g(e) \equiv 0(p^{2\sigma}) \not\equiv 0(p^{2\sigma+1})$, we have $\lambda \leq 2\sigma$. As a consequence of $\lambda \leq 2\sigma < \alpha$ and (68) we are then able to state

LEMMA 19. A necessary and sufficient condition that $\lambda > \lambda_0$ is that $x = e$ shall be a simultaneous solution of (67) with $\sigma = Y/3$, and of

$$(69) \quad H(x) = r(x) + 2h(x)g(x) \equiv 0(p^{2\lambda}).$$

Before proceeding to our final result we shall prove

LEMMA 20. The integer G of (66) is a cubic residue of p if and only if D_0 is a cubic residue of p .

For, by (65), (66) we have $G^2 \equiv 8a^3D_0(p)$ and the desired result follows at once.

We proceed now to the explicit determination of λ . Let e_0 be the unique solution mod p^σ of (67) with $\sigma = Y/3$. We then have

$$(70) \quad h(e_0) = h_0p^\sigma, \quad g(e_0) = g_0p^{2\sigma}, \quad r(e_0) = r_0p^Y, \quad r_0 \not\equiv 0(p),$$

for quotients h_0, g_0, r_0 . In fact by (1:14), (66) and (70), we have

$$(71) \quad 4ar_0 = A_0h_0p^\mu - G, \quad \mu = \alpha + \sigma - \gamma = \alpha - 2\sigma.$$

Let us now write

$$(72) \quad e = e_0 + kp^\sigma.$$

Then $H(e)$ of (69) may be developed in a Taylor expansion as in (9), (10). The result of substituting (70) in (10) then is

$$(73) \quad \begin{aligned} H(e_0) &= (r_0 + 2g_0h_0)p^\gamma, & H'(e_0) &= A_0p^\alpha - Cp^{\alpha_0} + 3h_0^2p^{2\sigma}, \\ \frac{H^{(2)}(e_0)}{2!} &= 12ah_0p^\sigma, & \frac{H^{(3)}(e_0)}{3!} &= 16a^2. \end{aligned}$$

Combining (73) with (9), we have

$$(74) \quad H(e) = p^\gamma \left\{ (r_0 + 2g_0h_0) + (A_0p^\mu - Cp^{\alpha_0+\sigma-\gamma} + 3h_0^2)k + 12ah_0k^2 + 16a^2k^3 \right\}.$$

We shall again call the expression within the brace of (74) $G(k)$.

We multiply $G(k)$ by $4a$ and make the substitution

$8ag_0 = h_0^2 - Cp^{\alpha_0-2\sigma}$, as well as that of (71). Then we obtain

$$(75) \quad \begin{aligned} 4aG(k) &= -G + A_0h_0p^\mu + h_0(h_0^2 - Cp^{\alpha_0-2\sigma}) + A_0p^\mu(4ak) \\ &\quad - 4akCp^{\alpha_0+\sigma-\gamma} + 48a^2k^2h_0 + 64a^3k^3. \end{aligned}$$

On regrouping the terms of (75) we get

$$(76) \quad 4aG(k) = -G + A_0p^\mu(4ak + h_0) - Cp^{\alpha_0-2\sigma}(4ak + h_0) + (4ak + h_0)^3.$$

We have already seen that $3\alpha_0 > 2\gamma = 6\sigma$, so that $\alpha_0 > 2\sigma$.

But from (62), $\alpha \geq \alpha_0$ so that $\mu = \alpha - 2\sigma > 0$. Finally we shall write

$$(77) \quad 4ak + h_0 = y,$$

and then (76) implies

$$(78) \quad 4aG(k) \equiv -G + y^3(p), \quad 4aG'(k) \equiv -3y^2(4a) \pmod{p}.$$

We then have trivially $G(k) \equiv 0(p)$ if and only if G is a cubic residue of p and then obviously $G'(k) \not\equiv 0(p)$. We may then conclude that $G(k) \equiv 0(p^\sigma)$ if and only if G of (66), and hence D_0 , is a cubic residue of p . It follows that $H(e) \equiv 0(p^{4\sigma})$, so that $\lambda = 2\sigma$. We shall state our results in

THEOREM 9. Let $3\alpha > \delta$, and $\gamma = 3\sigma$ for σ an integer, hold. Then $\lambda = 2\sigma$ if and only if D_0 of (1:17) is a cubic residue of p while otherwise $\lambda = \lambda_0$ of (43). In the former case, a corresponding solution of (1:2) is given by the first of (70), together with (72), (77) and

$$(79) \quad y^3 \equiv G(p).$$

If D_0 is a cubic non-residue of p , it is sufficient to take e to be a solution of (67) with $\sigma \geq \gamma/3$.

This completes the consideration of the case $3\alpha > \delta$.

5. A consequence of $\alpha = 0$. We state the result of this section at once in

THEOREM 10. Let $\alpha = 0$. Then the integer $\lambda = \gamma$ and the solution $x = e$ of (1:2) may be chosen to be a root of

$$(80) \quad r(x) \equiv 0(p^\delta).$$

For, if e is chosen as a solution of (71), (1:13) together with $\alpha = 0$ imply that $g(e) \equiv 0(p^\delta)$. These results when substituted into (1:5) and (1:7) require that $f'(e) \equiv 0(p^\delta)$, $f(e) \equiv 0(p^\delta)$, $\delta \geq 2\gamma$. Hence $\lambda = \gamma$ and our theorem is proved.

CHAPTER III

SOLUTION OF CONGRUENCES FOR THE CASE

WHERE p DIVIDES ab UNDER HYPOTHESES

IMPLYING $\alpha = 0$

We first derive the hypotheses, in addition to $ab \equiv 0(p)$, which imply $\alpha = 0$. The first of our results is that of

LEMMA 1. Suppose p divides a but is prime to bc . Then the integer α of (1:18) is zero.

The hypothesis of Lemma 1 combined with (1:3) evidently requires that $p \neq 3$. It then follows at once from (1:6) that $\alpha = 0$.

We likewise have

LEMMA 2. If the prime $p \neq 2$ is prime to a but divides both b and c , then the integer α of (1:18) is zero.

In both of the preceding lemmas we have made hypotheses implying $\alpha = 0$. In addition we shall write a combination of the hypotheses on a in the form

$$a = a_0 p^{\nu}, \quad \nu \geq 0.$$

We then pass to the final result of this chapter, which we state as

THEOREM 1. Let the hypotheses of Lemmas 1, 2 hold, so that α is zero. Then $\lambda = \gamma$ and a corresponding solution of (1:2) is given by a root of

$$r(x) \equiv 0(p^{\delta+2\nu}).$$

The proof is entirely analogous to that of Theorem 2:10.

CHAPTER IV

CONGRUENCE SOLUTIONS UNDER THE HYPOTHESIS THAT

p DIVIDES a AND c BUT NOT b

1. A special condition. Our hypotheses imply that $D \equiv -27b^2(p^2)$, so that $D \equiv 0(p^2)$ if and only if $p = 3$. Thus the hypotheses of this chapter may be stated in the form

$$(1) \quad p = 3, \quad a \equiv 3^f a_0, \quad c \equiv 3^{\tau} c_0, \quad p, \tau > 0.$$

The further development of this chapter is similar to that of Chapter II. Our subdivision into sections will here be based, however, on the relative magnitude of 3α to $\delta + 3p$. Before undertaking the main problem, we shall require the results of

2. Some preliminary lemmas.

LEMMA 1. Let either $\rho > 1$ or $\tau > 1$ hold. Then $\alpha = 2$.

This result is immediate from (1) and (1:6).

LEMMA 2. The exponent δ of (1:17) satisfies $\delta \geq 3$.

Moreover the hypothesis $3\alpha \geq \delta + 3p$ implies $\rho = 1$.

The first statement follows at once from (1) applied to (1:3). Next, assume $\rho > 1$. Then by Lemma 1 we have $\alpha = 2$ which contradicts $3\alpha \geq \delta + 3p$.

3. Consequences of the condition⁹ $0 < 3\alpha < \delta + 3p$. Our

⁹In the author's doctoral dissertation it was found more practicable to subdivide this section into three parts according as $\rho > 1$, $\tau > 1$ and $\rho = \tau = 1$. However, both the preliminary and final results in these parts are similar, and what follows is a compilation of the common results. For the original detailed development, refer to pp. 28-47 of "Integral domains in quartic fields" in the University of Chicago library.

first result is the analog of Theorem 2:1 and may be stated as

THEOREM 1. The numbers C, G defined by

$$(2) \quad A - 2ab^{-1}B = C3^{\alpha}$$

$$(3) \quad 3bA - 4aB = G3^{3\alpha/2}$$

are integral and prime to three. Moreover $\alpha = \beta$ is even.

The result $\beta = \alpha$ follows at once from (1:11) in view of the hypothesis $3\alpha < \delta + 3\rho$. Thus C is integral and prime to 3, since A is exactly divisible by 3^{α} . We then obtain (3) and the fact that α is even by applying (2) to (1:12).

Henceforth we shall assume unless otherwise stated that $\delta \geq 5$. We then pass to the proof of

LEMMA 3. If ρ or τ exceed unity, we have $\alpha = 2$. However if $\rho = \tau = 1$, the even exponent α satisfies $\alpha \geq 4$.

The first statement has been proved in Lemma 1. Assume $\rho = \tau = 1$ and that $\alpha = 2$. Note that (1:12) implies $C \equiv 1(3)$, while (2) gives $A_0 \equiv C \equiv 1(3)$. But then $A_0 = b^2 - 6a_0^3 - 8a_0c_0$, $A_0 \equiv b^2 - 8a_0c_0 \equiv 1(3)$, if and only if $a_0c_0 \equiv 0(3)$, a contradiction, proving the lemma.

We now define λ_0 exactly as in (2:3) and may then prove, analogously to Lemma 2:3, the result of

LEMMA 4. The integer λ has λ_0 as a lower bound. Equations (1:2) are satisfied for $\lambda = \lambda_0$ when we take $x = e$ to be a solution of

$$(4) \quad r(x) \equiv 0(3^{\delta+2\rho}).$$

We then proceed to the analog of Theorem 2:2. It is

THEOREM 2. Let $\delta \geq 7$. Then the integer $\lambda \geq \alpha$. In case $\alpha = 2$, equations (1:2) may be satisfied for $\lambda = \alpha$ by choosing

$x = e$ to be a solution of (4). In case $\alpha \geq 4$ the solution $x = e$ may be chosen in the form

$$(5) \quad e = e_0 + k3^{\alpha/2}.$$

The integer e_0 of (5) is given as a solution of

$$(6) \quad r(x) \equiv 0(3^{3\alpha/2+1}),$$

while k is given as a solution of

$$(7) \quad 4a_0x + h_0 \equiv 0(3),$$

with h_0 defined by $h(e_0) = h_0 3^{\alpha/2}$.

For the case $\alpha = 2$, our conclusion follows at once from Lemma 4. Let $\alpha \geq 4$, so that $\rho = \tau = 1$. Note that the conditions (5), (6), (7) on e imply that

$$(8) \quad r(e) = r3^{3\alpha/2}, \quad g(e) = g3^{\alpha}, \quad h(e) = h3^{\alpha/2}, \quad rgh \not\equiv 0(3).$$

By means of (8), our result may then be established by showing that $4a^2f(e) \equiv 0(3^{2\alpha+2})$. This is accomplished by applying a Taylor development in powers of k to $4a^2f(e)$ of (1:8). It then follows that $4a^2f(e) \equiv 0(3^{2\alpha+2})$ if and only if k satisfies (7).

Note that as a result of Lemma 4 and Theorem 2 we have demonstrated λ_1 of (2:13) as a lower bound on λ in case $\delta \geq 7$, and λ_0 as a lower bound on λ in the remaining cases. Moreover, recall that for $\delta \geq 7$ and $\alpha = 2$, we have $\lambda_0 \geq 2$ so that λ_1 actually is λ_0 . However this distinction is not necessary and will not be made again.

We now derive, in case $\lambda > \lambda_1$, some necessary conditions on $g(e)$, $r(e)$, and $h(e)$ in the simple

LEMMA 5. Suppose $\lambda > \lambda_1$. Then if we write $\phi = \alpha/2$

we must have

$$(9) \quad g(e) = g3^\varepsilon, \quad h(e) = h3^\varphi, \quad r(e) = r3^{\varepsilon+\varphi}, \quad rgh \neq 0(3), \quad \varepsilon \geq \lambda.$$

The fact that $g(e) = g3^\varepsilon$, $\varepsilon \geq \lambda$, has already been pointed out in (1:19). The remaining two relations on $h(e)$ and $r(e)$ are then trivial consequences of (1:10) and (1:13) respectively.

We now state the analog of Lemma 2:7. It is

LEMMA 6. An upper bound on λ is given by $\lambda \leq \gamma - \alpha/2$.

Moreover the exponent ε of (9) satisfies $\varepsilon \leq \gamma - \alpha/2$.

The proof is very similar to that of Lemma 2:7, and follows from (1:16) by assuming $\varepsilon \geq \gamma - \varphi + 1$.

Next, let us dispose of the case $3\alpha \geq \delta$. Our result is contained in

LEMMA 7. Let $\delta + 3\rho > 3\alpha \geq \delta \geq 7$. Then the integer $\lambda = \alpha$, and an appropriate solution $x = e$ of (1:2) is given by (5), (6), (7).

The result is obvious from the fact that $\gamma - \alpha/2 \leq \alpha$ under the hypothesis of this lemma.

We now define the function

$$(10) \quad F(x) = 4AF_0(x),$$

for $F_0(x)$ defined by (1:16), and shall establish

LEMMA 8. Equations (1:2) are equivalent to

$$(11) \quad \begin{aligned} F(x) &= h(4A^2g^2 + 2Ar^2 - AaD) + g(12A^2r) \\ -3bA(16Ag^2 + 2r^2 - aD) &\equiv 0(3^\theta), \quad \theta = 2\lambda + 2\rho + 5\varphi, \\ r &= r(x), \quad h = h(x), \quad g = g(x) \equiv 0(3^\lambda). \end{aligned}$$

For the right side of (11)₁ is identically equal to $4AF_0(x)$ for $F_0(x)$ defined by (1:15) and (1:16).

As the final lemma of this section, we shall require

LEMMA 9. A necessary condition for $\lambda > \lambda_0$ when $\delta < 7$, or for $\lambda > \lambda_1$ when $\delta \geq 7$ is that $\varepsilon \equiv \gamma - \alpha/2$ in (9).

For, the assumption $\varepsilon < \gamma - \alpha/2$ leads to the result $F(x) \equiv 0(3^{2\varepsilon+2\alpha+2})$, exactly, giving $\lambda \leq \lambda_0$. This contradicts the hypothesis of the lemma.

We now state without proof the key theorem of this section, which is the analog of Theorem 2:4. It is

THEOREM 3. Let $\delta \geq 5$. Then the integer $\lambda = \gamma - \alpha/2$ if and only if both

$$(12) \quad \delta = 2\gamma,$$

$$(13) \quad D_0 + 1 \equiv 0(3), \quad \gamma = 3; \quad D_0 - 1 \equiv 0(3), \quad \gamma > 3,$$

hold. An appropriate solution $x = e$ of (1:2) is then given by a solution of

$$(14) \quad r(x) \equiv 0(3^\gamma) \not\equiv 0(3^{\gamma+1}).$$

If both (12) and (13) are not simultaneously satisfied, we have λ given by

$$(15) \quad \lambda = \lambda_0, \quad \delta < 7; \quad \lambda = \lambda_1, \quad \delta \geq 7.$$

An appropriate solution $x = e$ of (1:2) is then given by (4) for the case $\delta < 7$, and either (4), or (5), (6), (7) in case $\delta \geq 7$.

We have yet to consider the cases $\delta = 4, 3$ under $3\alpha < \delta + 3\rho$. This implies $\alpha = 2$ in both cases, and thus that either τ or ρ exceeds unity. Note next, that $\lambda > 0$ in (1:2) if and only if

$$(16) \quad e = -b, \quad f(-b) = b^4 + a_0 b^2 3^\rho - b^2 + c_0 3^\tau \equiv 0(9).$$

We dispose first of the case $\delta = 4$ in

THEOREM 4. Let $\delta = 4$. Then the integer λ is zero.

For if $\rho \geq 2$ we have by (1:3) $\tau = 1$ and $c_0 \equiv 1(3)$. But then $f(-b) \equiv 0(9)$ of (16) is impossible, so that $\lambda = 0$.

Next let $\tau \geq 2$. It follows that $\rho = 1$, $a_0 \equiv -1(3)$, and hence that (16) is impossible. Our theorem is thus proved.

We now consider $\delta = 3$ with $3\alpha < \delta + 3\rho$, so that $\rho > 1$ and $c_0 \not\equiv 1(3)$ both hold. We then obtain our final

THEOREM 5. Let $\delta = 3$. Then $\lambda = 1$ if and only if one of conditions

$$(17) \quad c_0 \equiv -1(3), \quad b \equiv \pm 2(9); \quad c_0 \equiv 0(3), \quad b \equiv \pm 1(9)$$

holds. Then $e = -b$ is an appropriate solution of (1:2). If (17) is unsatisfied λ is zero.

4. Results for the case $3\alpha = \delta + 3\rho$. Recall that by Lemma 2 we have shown that $\rho = 1$ under the hypothesis of this section. The development of this section is analogous to that of Section 2:3. Thus, similarly to Lemma 2:10, we have

LEMMA 10. Let $\delta > 3$. Then the integer

$$\beta = \alpha \equiv \delta + 1(2),$$

and equation (2:1) holds for integral $C \not\equiv 0(3)$.

We shall assume until otherwise stated that $\delta > 3$. Then as a result of (1:12) and $3\alpha = \delta + 3$, we have

$$(3bA - 4aB)^2 = (8a_0^3D_0 + A_0^2C)3^{\delta+3},$$

which clearly implies that

$$(18) \quad 8a_0^3D_0 + A_0^2C = G_0^23^w, \quad G_0 \not\equiv 0(3),$$

where ψ has the form 2ν or $2\nu + 1$ according as δ is odd or even.

Let us now define the integer

$$(19) \quad \delta_0 = \left[\frac{\delta + 4}{2} \right] = \gamma + 2.$$

We then have analogously to Theorem 2:5,

THEOREM 6. The equation

$$(20) \quad 3ba - 4aB = G_0 3^{\delta_0 + \nu}, \quad G_0 \neq 0(3),$$

holds for G_0, ν defined in (18), δ_0 in (19).

Let us now define the integers λ_0 and λ_1 according to

$$(21) \quad \lambda_0 = \left[\frac{\gamma - 1}{2} \right], \quad \lambda_1 = \left[\gamma/2 \right].$$

We then proceed to the analogs of Lemmas 2:11, 2:12 and 2:13.

LEMMA 11. The integer λ satisfies $\lambda_0 \leq \lambda \leq \alpha - 1$.

For $\lambda \geq \alpha$ requires $g(e) \equiv 0(3^\alpha)$. This condition applied to (1:8) leads to $\lambda = \lambda_0$ or $\lambda = \lambda_1$, contradicting $\lambda \geq \alpha$.

LEMMA 12. The integer $\lambda > \lambda_0$ only if $x = e$ satisfies

$$(22) \quad h(x) \equiv 0(3^\sigma), \quad \sigma = \left[\frac{\alpha + 1}{2} \right].$$

Lemma 12 also follows from (22) applied to (1:8) and (1:10). In view of $\lambda < \alpha$ and (22) we obtain the analog of Lemma 2:13.

LEMMA 13. Equations (1:2) are equivalent, for maximum λ , to

$$(23) \quad \begin{aligned} g(x) &\equiv 0(3^\lambda), \\ F(x) &= -3^{2\alpha-1} + Bb^{-1}g(x) + xH(x) \equiv 0(3^{2\lambda+2}), \end{aligned}$$

where $H(x)$ is given by (2:8).

We now proceed to the actual determination of λ , with $x = e$

a solution of (22). Hence e is of the form

$$(24) \quad e = e_0 + k3^{\sigma-1},$$

with e_0 the unique solution mod $3^{\sigma-1}$ of (22). We may then obtain in the usual manner the divisibility properties expressed by

$$(25) \quad h(e_0) = h_0 3^{\sigma}, \quad g(e_0) = g_0 3^{\alpha-1}, \quad r(e_0) = r_0 3^{\alpha+\sigma-1},$$

with analogous properties on the functions $h(e)$, $g(e)$, $r(e)$.

Note that with e chosen as in (24), we have

$$(26) \quad F(e) \equiv eH(e) \pmod{3^{2\alpha-1}}.$$

Application of a Taylor development to $H(e)$ then leads to

$$(27) \quad H(e) = 3^{\gamma+1} \left\{ (r_0 + 2g_0h_0) + (h_0^2 3^4 + A_0 - C)k + 4a_0h_0k^2 3^{4+1} + 16a_0^2 k^3 3^4 \right\}, \quad \mu = 2\sigma - \alpha.$$

We also have the analogs of equations (2:47), (2:52) and (2:54). They are

$$(28) \quad 4a_0r_0 = A_0h_0 - G_0p^{\nu}, \quad 8a_0g_0 = h_0^2 p^{\mu} - C,$$

and

$$(29) \quad A_0 + 2C = b^{-1}G_0p^{\sigma+\nu},$$

and are derived by methods analogous to those of pages 18 and 19.

We then modify $4a_0H(e)$, for $H(e)$ given by (27), by using (28)

and (29) and obtain

$$(30) \quad 4a_0H(e) = 3^{\gamma+1}M(y), \quad M(y) \equiv 3^4 y^3 - 3Cy - G_0 3^{\nu} \pmod{3^{\sigma+\nu}},$$

where

$$(31) \quad y = 4a_0k + h_0.$$

Moreover, for the case α odd with e chosen to satisfy

(22), we have $8a_0g(e) = h^23^\alpha - C3^{\alpha-1}$, $a_0 \equiv 1(3)$. Also $B_0b^{-1} \equiv A_0 \equiv C(\text{mod } 3)$. It thus follows that

$$8a_0[Bb^{-1}g(e) - 3^{2\alpha-1}] \equiv [-C^2 + 1]3^{2\alpha-1}(\text{mod } 3^{2\alpha}) \equiv 0(3^{2\alpha}),$$

so that by (23), we have

$$(32) \quad F(e) \equiv eH(e)(\text{mod } 3^{2\alpha}).$$

First suppose α odd and $\nu = 0$. Then $\mu = 1$ and evidently $M(y) \not\equiv 0(3)$, $\lambda = \lambda_0$ of (21). Next let $\nu > 0$. Then combining (30) and (32), we have

$$(33) \quad \begin{aligned} 4a_0F(e) &\equiv e3^{\gamma+2}N(y)(\text{mod } 3^{2\alpha}), \\ M(y) &= 3N(y), \quad N(y) = y^3 - Cy - G_03^{\nu-1}. \end{aligned}$$

Assume that $\nu = 1$ in (33). Obviously then $N(y) \equiv 0(3)$ implies $y \not\equiv 0(3)$ and

$$(34) \quad C + 1 \equiv 0(3).$$

But in this case $N'(y) \equiv -C(\text{mod } 3) \not\equiv 0(3)$, so that it is evident that $N(y) \equiv 0(3)$, $N'(y) \not\equiv 0(3)$ are simultaneously satisfied. Accordingly $N(y) \equiv 0(3^\sigma)$ is solvable and hence $\lambda = \alpha - 1$ if and only if (34) holds.

The case α odd, $\nu > 1$ in (33) is trivial and is stated along with our other results in

THEOREM 7. Let $3\alpha = \delta + 3$ be odd. Then if $\nu = 0$, the integer $\lambda = \lambda_0$ and an appropriate solution of (1:2) is given by (22).

If $\nu = 1$, we have $\lambda = \alpha - 1$ if and only if (34) holds for C defined as in (2:1). The appropriate solution $x = e$ is given by (24), (31) and $y \not\equiv 0(3)$. If (34) does not hold then $\lambda = [\gamma/2]$,

and an appropriate solution is given by (23).

If $\nu > 1$, then $\lambda = \alpha - 1$ always. The solution $x = e$ is then given by (24), (31) and $y \equiv 0(3)$.

We now consider $3\alpha = \delta + 3$ even so that δ is of the form $2Y + 1$. Combining (26) and (30) we see that

$$(35) \quad \begin{aligned} 4a_0 F(e) &= e_0 3^{Y+1} P(k), \quad P(k) \equiv M(y) \pmod{3^{2\alpha-Y-2}}, \\ M(y) &= y^3 - 3Cy - G_0 3^\nu. \end{aligned}$$

We shall need an extension of the result mentioned on page 10, which is also a special case of the Hensel Lemma. It is

LEMMA 14. Let the congruence equations $P(x) \equiv 0(9)$, $P'(x) \equiv 0(3) \not\equiv 0(9)$, $P''(x) \equiv 0(3)$ be simultaneously satisfied for a solution $k_0 \pmod{9}$. Then $P(x) \equiv 0(3^5)$ is solvable for all ξ .

The proof is made by means of an induction. The lemma is true for the case $\xi = 2$. If $k_1 \equiv k_0(9)$ is a solution of $P(x) \equiv 0(3^5)$, it follows simply by a Taylor expansion on $P(k)$ that a solution of $P(x) \equiv 0(3^{\xi+1})$ of the form $k \equiv k_1(3^{\xi-1})$ exists, establishing our lemma.

We shall now deal with the case $\nu = 0$ in (35) and show that a solution of $M(y) \equiv 0(9)$, $M'(y) \equiv 0(9)$ cannot exist simultaneously. For, if so $M(y) \equiv 0(3)$ and $y^2 - C \equiv 0(3)$ would be simultaneously satisfied, requiring that the discriminant

$$(36) \quad G_0^2 - 4C^3 \equiv 0(3).$$

But we have by (18), $8a_0^3 D_0 + A_0^2 C = G_0^2$ with $A_0 \equiv C(3)$. The latter together with (36) implies that $8a_0^3 D_0 \equiv 0(3)$, an impossibility. Thus for $\nu = 0$, a solution of $M(y) \equiv 0(9)$ satisfies also $M'(y) \equiv 0(3) \not\equiv 0(9)$, $M''(y) \equiv 0(3)$. However a solution of $M(y) \equiv 0(9)$ exists only if $y \equiv G_0(3)$, and hence if and only if

$$M(G_0) = G_0^3 - 3CG_0 - G_0 = G_0(G_0^2 - 1 - 3C) \equiv 0(9).$$

The latter is equivalent to

$$(37) \quad G_0^2 - 1 - 3C \equiv 0(9).$$

The preceding discussion establishes the conditions of Lemma 14 provided (37) holds, so that $P(k) \equiv 0(3^{\sigma+1})$ is solvable and $\lambda = \alpha - 1$ under (37).

Suppose next that $\nu = 1$ in (35). We have $M(y) \equiv 0(3)$ if and only if $y \equiv 0(3)$. But then $M(y) \equiv 0(3) \not\equiv 0(9)$ and a similar statement holds for $P(k)$. Thus we have $\lambda = \lfloor \gamma/2 \rfloor$.

Finally assume $\nu > 1$ in (35). Again $M(y) \equiv 0(9)$ if and only if $y \equiv 0(3)$. Then by (35) we also have $M'(y) \equiv -3C \pmod{9}$, $M''(y) \equiv 0(3)$, with similar statements for $P(k)$, $P'(k)$, $P''(k)$. Thus by Lemma 14, $P(k) \equiv 0(3^{\sigma+1})$ is solvable and we have proved

THEOREM 8. Let $3\alpha = \delta + 3$ be even. Then if $\nu = 0$ the integer $\lambda = \alpha - 1$ if and only if (37) holds, and $\lambda = \lfloor \gamma/2 \rfloor$ otherwise. The solution $x = e$ of (1:2) is then given by (23), (24) (31) and $y \equiv G_0(3)$.

Let $\nu > 0$ hold. Then the exponent $\lambda = \alpha - 1$ if and only if $\nu > 1$, while $\lambda = \lfloor \gamma/2 \rfloor$ otherwise. The corresponding solution $x = e$ of (1:2) is given by (23), (24), (31) and $y \equiv 0(3)$.

In concluding this section we must dispose of the case $\delta = 3$. We do this in

THEOREM 9. Let $\delta = 3$, $\rho = 1$, and $\alpha = 2$. Then the exponent $\lambda = 1$ if and only if

$$(38) \quad b^2 - 1 + a + c \equiv 0(9),$$

while $\lambda = 0$ otherwise. The corresponding solution of (1:2) in case (38) holds is given by $e = -b$.

The proof follows at once from (16) on observing that the terms $b^4 - b^2 = b^2(b^2 - 1) \equiv b^2 - 1(9)$.

We now proceed to

5. Conclusions when $3\alpha > \delta + 3\rho$. Again, Lemma 2 implies that $\rho = 1$ under the hypothesis of this section. We define the integer α_0 as in (2:62), and clearly, we then have

LEMMA 15. If $\alpha \neq \beta$, the integer δ of (1:17) is given by $\delta = 2\alpha_0 - 1$. If $\alpha = \beta = \alpha_0$ then $\delta \geq 2\alpha - 1$. Moreover we have in either case $3\alpha_0 > \delta + 3$.

A further immediate result is then stated in

LEMMA 16. The number C defined by

$$(39) \quad A - 2ab^{-1}B = C3^{\alpha_0},$$

is integral

Then analogously to Theorem 2:8 we have

THEOREM 10. Let $3\alpha > \delta + 3 > 6$. Then $\delta = 2\gamma + 1$ and

$$(40) \quad 3bA - 4aB = G3^{\gamma+2}, \quad G \not\equiv 0(3),$$

holds for integral G. Also the integer $2a_0D_0$ is a quadratic residue of three.

We then pass at once to

LEMMA 17. Let $3\alpha > \delta + 3 > 6$. Then the exponents α, β of (1:18) satisfy $\alpha \geq 3, \beta \geq 3$, so that

$$(41) \quad a_0 \equiv -c_0 \equiv 1(3).$$

Furthermore, we have

$$(42) \quad D_0 \equiv -1(3).$$

Relation (41) follows at once from $\alpha \geq 3, \beta \geq 3$ applied to (1:6), while (42) follows from the final statement of Theorem 10 and $a_0 \equiv 1(3)$.

Our next five lemmas are then simple analogs of Lemmas 2:16, 2:17, 2:18, 2:19 and 2:20. They are

LEMMA 18. Let $\delta > 3$. Then the integer λ satisfies the inequality $\alpha_0 > \lambda \geq \lambda_0 = [\gamma/2]$.

LEMMA 19. A necessary condition that $\lambda > \lambda_0$ is that e shall be taken to be a root of

$$(43) \quad h(x) \equiv 0(3^\sigma) \not\equiv 0(3^{\sigma+1}), \quad \gamma + 2 - \alpha_0 < \sigma \leq \left[\frac{\alpha_0 - 1}{2} \right].$$

LEMMA 20. Let $3\alpha > \delta + 3 > 6$. Then $\lambda > \lambda_0$ only if $\gamma + 2 \equiv 0(3)$, and we choose σ of (43) to satisfy $\gamma + 2 = 3\sigma$. If $\gamma + 2 \not\equiv 0(3)$, then $\lambda = \lambda_0$ and an appropriate solution $x = e$ of (1:2) is obtained by taking e to be a solution of (43) with $3\sigma > \gamma + 2$.

Lemma 20 disposes of the cases $\gamma + 2 \not\equiv 0(3)$ and we shall henceforth confine ourselves to the case $\gamma + 2 = 3\sigma$. Then by (43), (1:10), we have $g(e) \equiv 0(3^{2\sigma-1}) \not\equiv 0(3^{2\sigma})$ and may pass to

LEMMA 21. A necessary and sufficient condition that $\lambda > \lambda_0$ is that $x = e$ be a simultaneous solution of (42) with $\sigma = (\gamma + 2)/3$, and of

$$(44) \quad F(x) = -3^{4\sigma-1} + xH(x) \equiv 0(3^{2\lambda+2}), \quad \lambda \leq 2\sigma - 1,$$

for $H(x)$ as in (2:8).

The analog of Lemma 2:20 is

LEMMA 22. The integer G of (40) is a cubic residue of nine if and only if $D_0 \equiv -1(9)$.

In proof, G is a cubic residue of nine if and only if $G^2 \equiv 1(9)$. Moreover $3\alpha > \delta + 3 = 2(\gamma + 2) = 6\sigma$ implies $3\alpha \geq \delta + 6$. Hence by (1:12) and (40) we have $G^2 \equiv 8a_0^3 D_0(3^3)$, from which, by $a_0 \equiv 1(3)$, we have our desired result.

We have now established all the necessary preliminary results and shall proceed to our final results for this case. Our solution $x = e$ must be a solution of (43) with $\sigma = (\gamma + 2)/3$, and our method is very closely analogous to that of pages 25 and 26. Thus we have (24) with e_0 the unique solution mod $3^{\sigma-1}$ of (43), and arrive at

$$(45) \quad \begin{aligned} H(e) &= 3^{3\sigma-1}G(k), \\ 4a_0G(k) &\equiv -G - 3^{4_0+1}Cy + y^3 \pmod{3^\sigma}, \quad \mu_0 = \alpha_0 - 2\sigma, \end{aligned}$$

with y given by (31). Combining (44) and (45) we obtain trivially

$$(46) \quad \begin{aligned} 4a_0F(e) &= 3^{3\sigma-1}P(k), \quad P(k) \equiv e_0M(y) \pmod{3^\sigma}, \\ M(y) &= y^3 - 3^{4_0+1}Cy - G, \quad \mu_0 = \alpha_0 - 2\sigma. \end{aligned}$$

But then since $\gamma + 2 = 3\sigma$, $\gamma \geq 2$, we have $\sigma \geq 2$. Moreover we have also $3\alpha_0 > \delta + 3 = 6\sigma$ so that $\mu_0 > 0$. Thus we have

$$P(k) \equiv e_0(y^3 - G) \pmod{9}, \quad P'(k) \equiv 4a_0e_0 \cdot 3y^2 \pmod{9},$$

so that $P(k) \equiv 0(9)$ if and only if G is a cubic residue of nine. Then also $P'(k) \equiv 0(3) \not\equiv 0(9)$ and Lemma 14 enables us to conclude that $P(k) \equiv 0(3^{\sigma+1})$ is solvable. In the contrary case $y^3 - G \equiv 0(3) \not\equiv 0(9)$ and in this case (44) and (46) show that $\lambda = [\gamma/2]$. We have thus proved

THEOREM 11. Let $3\alpha > \delta + 3 > 6$ and $\sigma = (\gamma + 2)/3$, for integral σ . Then the integer $\lambda = 2\sigma - 1$ if and only if $D_0 \equiv -1(9)$ while otherwise $\lambda = [\gamma/2]$. The solution $x = e$ of (1:2) is then given by (43), (24), (31) and $y^3 - G \equiv 0(3)$.

There remains now only the case $\delta = 3$. But then the hypothesis $3\alpha > \delta + 3$ implies $\alpha \geq 3$, while Lemma 15 implies $\beta = 2$. Moreover $\alpha > \beta = 2$ implies $\rho = \tau = 1$ in (1) and

$$(47) \quad c_0 \equiv -a_0 \equiv 1(3),$$

which, together with (16), easily leads to

THEOREM 12. Let $3\alpha > \delta + 3 = 6$ so that (47) holds.

Then the integer $\lambda = 1$ if and only if $b \equiv \pm 1(9)$ and a corresponding solution of (1:2) is given by $e = -b$.

Finally, excluding the special cases arising when $\delta < 5$, our main results have been stated in Theorems 3, 7, 8 and 11. The results of the last three of these become simplified on noting that the maximum values of λ , namely $\alpha - 1$ and $2\sigma - 1$, are both equal to $\delta/3$.

CHAPTER V

SOLUTION OF CONGRUENCES WHEN $p \neq 2$

DIVIDES b BUT NOT ac

The hypothesis of this chapter justifies the notation

$$(1) \quad b = b_0 p^\nu, \quad (b_0, p) = 1, \quad \nu > 0.$$

It is evident from (1:3) and $p \neq 2$ that $a^2 - 4c \equiv 0(p)$. We thus define integers Q and σ according to

$$(2) \quad a^2 - 4c = Qp^\sigma, \quad Q \not\equiv 0(p),$$

and have at once, by virtue of (1:3),

LEMMA 1. If $\sigma \neq \nu$, then $\delta = 2\nu$, where ν is the lesser of σ, ν . If $\sigma = \nu$, then $\delta \geq 2\nu$. Conversely if $\delta > 2\nu$, then $\sigma = \nu$.

Note that (1:3) may be rewritten in the form

$$(3) \quad D = 16c(a^2 - 4c)^2 - 4ab^2(a^2 - 4c) + 2^7acb^2 - 27b^4,$$

as a consequence of which we have

LEMMA 2. Let $\delta > 2\nu$. Then the integer $-2a$ is a quadratic residue of p .

For the present, assume $\delta > 2\nu$. We then have by (1:6)

LEMMA 3. Let $\delta > 2\nu$. Then the exponent $\alpha = \beta$. Moreover we have

$$(4) \quad A_0 \equiv 2aQ, \quad B_0 \equiv 16b_0c(p^\nu).$$

We then easily derive

LEMMA 4. Let $\delta > 2\nu$. Then there always exists a simultaneous solution of

$$(5) \quad r(x) \equiv 0(p^{\delta-\nu}),$$

$$(6) \quad 2x^2 + a \equiv 0(p^\nu).$$

First, for the case $\delta \geq 3\nu$, we choose $x = e$ to be a solution of (5). It then follows from (1:13) that $g(e) \equiv 0(p^{\delta-2\nu})$,

$$(7) \quad g(e) = a(2e^2 + a) + 3be - Qp^\nu,$$

so that our result is immediate.

Next, when $3\nu > \delta > 2\nu$, choose $x = e$ to satisfy (6). Then

$$(8) \quad 2(A_0e - B_0)(A_0e + B_0) = A_0^2(2e^2 + a) - (A_0^2a + 2B_0^2),$$

holds, for $A_0^2a + 2B_0^2$ the discriminant mod p of $A_0e + B_0$, $2e^2 + a$.

Note also that

$$A_0^2a + 2B_0^2 \equiv 4a^3Q^2 + 2^9b_0^2c^2 \equiv 4a^3(Q^2 + 8ab_0^2)(\text{mod } p).$$

However by (3) and $3\nu > \delta > 2\nu$, we have $Q^2 + 8ab_0^2 \equiv 0(p^{\delta-2\nu})$, exactly, so that (6), (8) imply that $x = e$ satisfies (5)..

We now define the integers

$$(9) \quad \lambda_0 = \left\lfloor \frac{\delta - \nu}{2} \right\rfloor, \quad \lambda_1 = \lfloor \gamma/2 \rfloor$$

and proceed to the proof of

THEOREM 1. Let $\delta > 2\nu$ for ν defined by (1). Then $\lambda = \lambda_0$ of (9), and the corresponding solution $x = e$ of (1:2) is given by a simultaneous solution of (5) and (6).

For we have $\lambda \geq \lambda_0$ immediately upon writing

$$(10) \quad 4a^2f(x) = a^2(2x^2 + a)g(x) - 3bxg(x) + xr(x).$$

Next suppose $\lambda = \lambda_0 + 1$. We then require simultaneously,

$$(11) \quad g(x) \equiv 0(p^{\lambda_0+1}), \quad F_0(x) \equiv 0(p^{2\lambda_0+2+\nu}),$$

for $F_0(x)$ given by (1:15), (1:16). However, by (1:16) and

$r(x) \equiv 0(p^{\lambda_0+1})$, we would have

$$F_0(x) \equiv 2ax[r(x)]^2 - a^2xD \pmod{p^{2\lambda_0+2+\nu}}.$$

Thus $\lambda > \lambda_0$ requires $\delta = 2\gamma$, $r(x) \equiv 0(p^\gamma) \not\equiv 0(p^{\gamma+1})$, and hence $g(x) \equiv 0(p^{\gamma-\nu})$, exactly. But then $\lambda_0 \geq \gamma - \lfloor \frac{\nu+1}{2} \rfloor \geq \gamma - \nu$, so that $\lambda_0 + 1 > \gamma - \nu$, which contradicts (11)₁. This completes the proof.

We conclude this chapter by proving

THEOREM 2. Let $\delta = 2\gamma \leq 2\nu$. Then $\lambda = \lambda_1$ of (9) if and only if $-2a$ is a quadratic residue of p , and $\lambda = 0$ otherwise. In the former case, the solution $x = e$ of (1:2) is given by a solution of

$$(12) \quad 2x^2 + a \equiv 0(p^{\lambda_1}).$$

In proof, note that (1:2) is equivalent to

$$(13) \quad \begin{aligned} f'(x) &= 2x(2x^2 + a) + b_0p^\nu \equiv 0(p^\lambda), \quad \nu \geq \gamma, \\ 4f(x) &= (2x^2 + a)^2 + 4xb_0p^\nu - Qp^\sigma \equiv 0(p^{2\lambda}), \quad \sigma \geq \gamma. \end{aligned}$$

Accordingly $\lambda > 0$ if and only if $2x^2 + a \equiv 0(p)$ is solvable, that is, if and only if $-2a$ is a quadratic residue of p . Assume that this condition is satisfied so that (12) is solvable. Clearly, (13) then implies $\lambda \geq \lambda_1$. Next, suppose $\lambda \geq \lambda_1 + 1$. Then (13) requires

$$(14) \quad 2x^2 + a \equiv 0(p^{\lambda_1+1}), \quad 4b_0p^\nu x - Qp^\sigma \equiv 0(p^{2\lambda_1+2})$$

to have a simultaneous solution. This is impossible in view of the hypothesis $\delta \leq 2\nu$ in (3), and we have established our theorem.

CHAPTER VI

CONGRUENCE SOLUTIONS WHEN $p \neq 2$ DIVIDES BOTH a AND b

The first result of this chapter is a trivial consequence of (1:3) and our hypothesis. It is

LEMMA 1. Let p divide both a and b . Then the integer c is also divisible by p . Moreover $\lambda > 0$ if and only if

$$(1) \quad c \equiv 0(p^2).$$

The last statement of the lemma follows from (1:2). We shall henceforth assume $c \equiv 0(p^2)$ so that $\lambda > 0$. We then have at once

THEOREM 1. Let $a \equiv c \equiv 0(p^2)$. Then $\lambda = 2$ if and only if

$$(2) \quad b = b_0 p^2, \quad (b_0, p) = 1, \quad c = c_0 p^3,$$

holds, and then equations (1:2) are satisfied by choosing the solution $x = e$ as in

$$(3) \quad e = e_0 p,$$

with e_0 a solution of

$$(4) \quad b_0 x + c_0 \equiv 0(p).$$

If (2) is not satisfied, λ is unity.

Theorem 1 furnishes a complete statement of the results for all cases in which $a \equiv 0(p^2)$. We may henceforth restrict our attention to the condition

$$(5) \quad a = a_0 p, \quad a_0 \not\equiv 0(p),$$

together with $c \equiv 0(p^2)$, $b \equiv 0(p)$. Then introduction of the notation (5:1) leads to the result of

LEMMA 2. Let (1) and (5) hold so that $\lambda > 0$. Then

$\lambda \geq 2$ only if

$$(6) \quad b = b_0 p^2, \quad c = c_0 p^3,$$

and

$$(7) \quad b_0^2 - 4a_0c_0$$

a quadratic residue of p , or divisible by p . If these conditions are not satisfied, the integer λ is unity.

In view of Lemma 2, we shall henceforth assume

$$(8) \quad c \equiv 0(p^3), \quad b = b_0 p^\nu, \quad \nu \geq 2,$$

in addition to (5). We then have at once the following lemmas:

LEMMA 3. Let conditions (5), (8) hold. Then A, B of

(1:6) satisfy

$$(9) \quad A = A_0 p^3, \quad B = B_0 p^{\nu+2}, \quad A_0 B_0 \not\equiv 0(p).$$

LEMMA 4. Define the integer

$$(10) \quad \lambda_0 = \gamma - 2.$$

Then (1:2) is satisfied for $\lambda = \lambda_0$ when we take $x = e$ to be a solution of

$$(11) \quad r(x) \equiv 0(p^5).$$

We now investigate the existence of solutions of (1:2) for $\lambda = \lambda_0 + 1$. Our next result is a simple consequence of (1:5) and is stated in

LEMMA 5. The integer $\lambda > \lambda_0$ only if the solution of

(1:2) satisfies

$$(12) \quad r(x) \equiv 0(p^{\lambda+2}).$$

In particular, $\lambda \geq \lambda_0 + 1 = \gamma - 1$ only if the solution $x = e$ of (1:2) satisfies

$$(13) \quad r(x) \equiv O(p^{\gamma+1}).$$

Our final result is then contained in

THEOREM 2. The integer $\lambda = \gamma - 1$ if and only if the conditions

$$(14) \quad \delta = 2\gamma + 1, \quad -a_0 D_0$$

a quadratic residue of p , are both satisfied. The corresponding solution $x = e$ of (1:2) is given as a solution of

$$(15) \quad r(x) \equiv yp^{\gamma+1} \pmod{p^{\gamma+2}},$$

with y a solution of

$$4x^2 \equiv -a_0 D_0(p).$$

If both conditions of (14) do not hold simultaneously, we have $\lambda = \gamma - 2$ and the solution $x = e$ of (1:2) is then given by (11).

For, equations (1:2) with $\lambda \geq \gamma - 1$ are equivalent to

$$(13) \text{ and } F_0(x) \equiv O(p^{2\gamma+\nu+3}), \quad F_0(x) \text{ given by (1:15), (1:16).}$$

The latter equation is satisfied if and only if (14) and (15) are both satisfied. Comparison of (12) and (15) then evidently implies $\lambda = \gamma - 1$ exactly. Our theorem is thus proved.

CHAPTER VII

THE FINAL CASE $p = 2$

In the preceding five chapters, the techniques employed as well as the results obtained have been quite similar. Let $p \geq 0$ be defined by $a = a_0 p^f$. Then, for example, our results have been substantially: $\lambda = [(\delta - \alpha)/2]$ or $\lambda = \lambda_1$ of (2:13) when $3\alpha < \delta + 3p$, while $\lambda = \delta/3$ or $\lambda = [\gamma/2]$ when $3\alpha \geq \delta + 3p$. The main technique has been to replace (1:2) by a pair of equivalent equations, usually involving $r(x)$ and $F_0(x)$ of (1:15), (1:16). In the present chapter the similarity in method and results to those of the previous chapters also holds. Hence what follows represents an essential portion of the argument without repetition of details which have been sufficiently amplified in the foregoing chapters.

1. A preliminary lemma. We shall prove

LEMMA 1. The integer b is divisible by two

$$(1) \quad b = b_0 2^v, \quad v > 0.$$

For, note that (1:17) and the hypothesis of the present chapter imply that $D = D_0 2^\delta$, $\delta > 0$, where D has the form (1:3). Our result then follows from (1:3).

2. The determination for a odd. Our first result is that of

THEOREM 1. The integer λ is positive if and only if c is even.

Henceforth let us assume that c is even. This assumption

together with (1) leads us trivially to

LEMMA 2. The integer $\delta \geq 5$.

Before stating the final result of this section we shall need the analogs of Lemmas 6:3, 6:4. They are

LEMMA 3. The integers A, B of (1:6) satisfy

$$(2) \quad A = 2A_0, \quad B = 2^\nu B_0, \quad A_0 B_0 \not\equiv 0(2).$$

LEMMA 4. Equations (1:2) are satisfied for $\lambda = \gamma - 2$ when we take $x = e$ to be a solution of

$$(3) \quad r(x) \equiv 0(2^\delta).$$

We then pass to our final

THEOREM 2. Let $\delta \geq 6$. Then the integer $\lambda = \gamma - 1$ if and only if the conditions

$$(4) \quad \delta = 2\gamma, \quad D_0 + a + 2^\nu \equiv 0(4), \quad \nu > 0,$$

are satisfied. The corresponding solution $x = e$ of (1:2) is then obtained as a solution of

$$(5) \quad r(x) \equiv 0(2^{\gamma-1}) \not\equiv 0(2^\gamma).$$

If (4) is not satisfied, $\lambda = \gamma - 2$ and an appropriate solution of (1:2) is given by (3).

Let $\delta = 5$. Then $\lambda = 1$ if and only if $a \equiv 1(4)$, an appropriate solution of (1:2) being $e = 1$. If $a \equiv -1(4)$, λ is zero.

3. Evaluation of λ when a is even, c odd. Our first result is that for the case $D = D_0 2^4$, $D_0 \not\equiv 0(2)$. It is given in

THEOREM 3. Let $D \equiv 0(2^4) \not\equiv 0(2^5)$. This condition is equivalent to

$$(6) \quad b \equiv 2(4).$$

Then $\lambda = 1$ if and only if the condition

$$(7) \quad c - 1 \equiv a(4)$$

is satisfied. The solution $x = e$ of (1:2) is given by any odd number. If (7) is not satisfied, the integer λ is zero.

Theorem 3 disposes of the cases $b \equiv 2(4)$, and we shall henceforth consider only $b \equiv 0(4)$. We obtain the trivial

LEMMA 5. Let $b \equiv 0(4)$. Then the integer of (1:17) satisfies $\delta \geq 8$.

We next dispose of the case $\delta = 8$. We shall need

LEMMA 6. The condition $\delta = 8$ is equivalent to one of the sets of conditions

$$(8) \quad b = b_0 2^2, \quad a = 2a_0, \quad a_0 b_0 \not\equiv 0(4),$$

$$(9) \quad b \equiv 0(8), \quad a \equiv 0(4).$$

Our corresponding results on λ for the case $\delta = 8$ are then given by

THEOREM 4. Let $\delta = 8$. Then if (8) holds, $\lambda = 2$ if and only if

$$(10) \quad a + c \equiv 3(8),$$

while $\lambda = 1$ if and only if

$$(11) \quad a + c \equiv -1(8)$$

is satisfied. If neither (10) nor (11) holds, λ is zero.

If (9) holds, the integer $\lambda = 2$ if and only if

$$(12) \quad 1 + a + b + c \equiv 0(16),$$

while $\lambda = 1$ if and only if (12) is not satisfied, and

$$(13) \quad c + 1 \equiv 0(4)$$

holds. If neither (12) nor (13) holds, then λ is zero.

In every case for which $\lambda > 0$, an appropriate solution $x = e$ of (1:2) may be taken to be any odd number.

As a result of Theorem 4, we shall henceforth consider only $\delta > 8$. We are therefore excluding (8), (9) from further consideration. Thus there remain only the possibilities

$$(14) \quad b \equiv 0(8), \quad a = 2a_0, \quad a_0 \not\equiv 0(2),$$

$$(15) \quad b = 4b_0, \quad a \equiv 0(4), \quad b_0 \not\equiv 0(2),$$

and we dispose of (14) at once by means of the trivial

THEOREM 5. Let $\delta > 8$ and (14) hold. Then $\lambda = 1$ if and only if

$$(16) \quad c \equiv 1(4)$$

holds, while if (16) is not satisfied λ is zero.

We now have left only the condition (15), which we shall write in the form

$$(15a) \quad b = 4b_0, \quad a = a_0 2^p, \quad p \geq 2, \quad a_0 b_0 \not\equiv 0(2).$$

By means of (1:3) and (1:6) we then pass to the simple

LEMMA 7. Let (15a) hold. We then have $\delta \geq 9$ and also

$$(17) \quad A = 2^4 A_0, \quad B = 2^4 B_0, \quad A_0 B_0 \not\equiv 0(2).$$

Applying Lemma 7 to (1:13), we may state a lower bound on λ in

LEMMA 8. The exponent $\lambda \geq \gamma - 4$. Equations (1:2) are

satisfied for $\lambda = Y - 4$ if we choose $x = e$ to be a solution of

$$(18) \quad r(x) \equiv O(2^{\delta+2p}).$$

We now pass to the statement, without proof¹⁰ of the final results of this section. It is contained in

THEOREM 6. Let (15a) hold. Then $\lambda > Y - 4$ if and only if

$$(19) \quad \delta = 2Y + 1 \geq 11$$

holds. Assume (19) is valid. Then $\lambda = Y - 2$ if and only if one of

$$(20) \quad Y \geq 6, \quad D_0 + 1 + 2^{p-1}a_0 \equiv O(8),$$

$$(21) \quad Y = 5; \quad D_0 + 3 \equiv O(8), \quad p \geq 3; \quad D_0 + 3 + 2a_0 \equiv O(8), \quad p = 2,$$

is true. If (19) holds, but neither (20) nor (21) is satisfied, we have $\lambda = Y - 3$. In either case the appropriate solution $x = e$ of (1:2) is obtained as a solution of

$$(22) \quad r(x) \equiv O(2^Y) \neq O(2^{Y+1}).$$

If $\delta = 2Y$, then $\lambda = Y - 4$ and a corresponding solution of (1:2) is given as a solution of (18).

4. Consequences of the hypothesis a, b, c all even.

Our development in this section will follow that of Chapter VI somewhat closely. Thus our first two results are the analogs of Lemma 6:1 and Theorem 6:1. They are

LEMMA 9. Let the conditions $a \equiv b \equiv c \equiv O(2)$ hold.

¹⁰The proof of this is rather complicated. It is given fully in pp. 86-98 of the author's doctoral dissertation. Actually it was found advisable to make two separate arguments according as $p < Y - 3$ and $p \geq Y - 3$. The theorem as here stated, is a compilation of the results contained in Theorems 7:7, 7:8, 7:9 of the author's thesis.

Then the integer $\lambda > 0$ if and only if $c \equiv 0(2^2)$.

THEOREM 7. Let $a \equiv c \equiv 0(2^2)$. Then $\lambda = 2$ if and only if

$$(23) \quad b = b_0 2^2, \quad b_0 \not\equiv 0(2), \quad c \equiv 0(2^3)$$

holds, and then equations (1:2) are satisfied by choosing $e = 2e_0$ with e_0 a solution of

$$(24) \quad b_0 x + c_0 \equiv 0(2), \quad c = c_0 2^3.$$

Theorem 7 gives the complete solution in all cases for which $a \equiv 0(4)$. Throughout the remainder of this section we consider only

$$(25) \quad a = 2a_0, \quad a_0 \not\equiv 0(2)$$

along with $b \equiv 0(2)$, $c \equiv 0(2^2)$. Thus we state a partial analog of Lemma 6:2,

LEMMA 10. Let (25) hold and also $c \equiv 0(2^2)$ so that $\lambda > 0$. Then $\lambda \geq 2$ only if

$$(26) \quad b = b_0 2^2, \quad c = c_0 2^3,$$

and $\lambda = 1$ otherwise. Moreover if $b_0 \not\equiv 0(2)$, the integer λ is two.

In view of Lemma 10, we shall henceforth consider only

$$(27) \quad c \equiv 0(2^3), \quad b = b_0 2^\nu, \quad \nu \geq 3, \quad b_0 \not\equiv 0(2).$$

As consequences of (25) and (27), we have at once the following lemmas:

LEMMA 11. The exponent δ of (1:17) satisfies $\delta \geq 11$.

LEMMA 12. Let (25), (27) hold. Then the integers A, B of (1:6) satisfy

$$(28) \quad A = A_0 2^4, \quad B = B_0 2^{\nu+2}, \quad A_0 B_0 \not\equiv 0(2).$$

Moreover, application of (28) in the usual manner to (1:13) and (1:7) leads to

LEMMA 13. Let (25), (27) hold. Then equations (1:2) are satisfied for $\lambda = \gamma - 4$ when we take $x = e$ to be a solution of

$$(29) \quad r(x) \equiv 0(2^{\gamma}).$$

We now pass to the concluding theorem of this section,

THEOREM 8. The exponent $\lambda > \gamma - 4$ if and only if

$$(30) \quad \delta = 2\gamma + 1.$$

In fact, $\lambda = \gamma - 2$ if and only if one of the following conditions

$$(31) \quad \gamma \geq 6, \quad D_0 + a_0 + 2^{\gamma-1} \equiv 0(8),$$

$$(32) \quad \gamma = 5; \quad D_0 + a_0 \equiv 0(8), \quad \gamma = 3; \quad D_0 + a_0 + 2 \equiv 0(8), \quad \gamma > 3,$$

holds. If (30) holds but neither (31) nor (32) is satisfied then

$\lambda = \gamma - 3$. In either case an appropriate solution of (1:2) is obtained as a solution

$$(33) \quad r(x) \equiv 0(2^{\gamma}) \not\equiv 0(2^{\gamma+1}).$$

If $\delta = 2\gamma$, then $\lambda = \gamma - 4$ and a corresponding solution

$x = e$ of (1:2) is given as a solution of (29).

5. Summary of the results. We have been concerned with the determination of the denominator E of the set of all integers of the integral domain discussed in the Introduction. We shall now summarize our results on the values of λ , the exponent of the prime factors p of the denominator E . These results will be stated in the terms of δ , the maximum power of p dividing the discriminants D of the quartic equation $f(x) = 0$ defining the fields we are considering. Moreover δ has the form either 2γ or $2\gamma + 1$.

Thus in case $p = 2$, our results are those of

THEOREM 9. The exponent λ has one of the values $\delta - 1$, $\delta - 2$, $\delta - 3$, $\delta - 4$.

For the case $p \neq 2$, let us recall that we defined an exponent $\lambda_0 = [(\delta - 3\alpha/2)/2]$. The integer α has the meaning given by $A = A_0 p^\alpha$, for A a certain polynomial in the coefficients of $f(x)$ and A_0 prime to p . In Chapters II and IV, this definition of λ_0 was adequate since α was shown to be even. In order that our results may include those of Chapter VI where $\alpha = 3$, we extend this definition of λ_0 to

$$\lambda_0 = \left[\frac{\delta - \left[\frac{3\alpha}{2} \right]}{2} \right].$$

If then λ_1 be defined as the maximum of λ_0 and α , we have

THEOREM 10. The exponents λ on prime factors $p \neq 2$ of E have values given by one of the equations $\lambda = [(\delta - \alpha)/2]$, $\lambda = \lambda_1$, $\lambda = \delta/3$, $\lambda = [\delta/2]$, $\lambda = [(\delta - 1)/2]$.

VITA

Frank Lionel Martin was born in Montreal, Canada, on May 16, 1915. He received his elementary and high school education in the schools of Vancouver, Canada. In 1932 he entered the University of British Columbia at Vancouver, Canada, graduating in May, 1936, with the degree of Bachelor of Arts. During the next two years he was engaged in graduate study at the same University, and was awarded the degree of Master of Arts in 1938. He was in residence at the University of Chicago for seven quarters beginning with the Autumn Quarter of 1938. At the University of British Columbia he studied under Professors Richardson, Buchanan and Nowlan, and at the University of Chicago under Professors Bliss, Lane, Dickson, Albert, Barnard and Bartky. He is grateful to all these instructors, and especially to Professor Albert under whose direction this thesis was written.

